PCSecurityShield

SHIELD DELUXE 2013

Advanced Virus & Malware Protection

USER GUIDE

SHIELD DELUXE 2013

SHIELD DELUXE 2013
User's Guide

Published 2012.12.12

Legal Notice

Warning and Disclaimer. This product and its documentation are protected by copyright. The information in this document is provided on an “as is” basis, without warranty. Although every precaution has been taken in the preparation of this document, the authors will not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

This book contains links to third-party Websites that are not under the control of PCSecurityShield, therefore PCSecurityShield is not responsible for the content of any linked site. If you access a third-party website listed in this document, you will do so at your own risk. PCSecurityShield provides these links only as a convenience, and the inclusion of the link does not imply that PCSecurityShield endorses or accepts any responsibility for the content of the third-party site.

Trademarks. Trademark names may appear in this book. All registered and unregistered trademarks in this document are the sole property of their respective owners, and are respectfully acknowledged.

Table of Contents

Installation and Removal 1

1. System Requirements 2
1.1. Minimal System Requirements 2
1.2. Recommended System Requirements 2
1.3. Software Requirements 3

2. Preparing for Installation 4

3. Installing SHIELD DELUXE 2013 5
3.1. Step 1 - Introduction 5
3.2. Step 2 - Preparing Install 5
3.3. Step 3 - Registration 6
3.4. Step 4 - Choose View 7
3.5. Step 5 - Configure 8
3.6. Step 6 - Support Options 12
3.7. Step 7 - Confirm 12
3.8. Step 8 - Finish 13

4. Upgrade 14

5. Repairing or Removing SHIELD DELUXE 15

Getting Started 16

6. Overview 17
6.1. Opening SHIELD DELUXE 17
6.2. System Tray Icon 17
6.3. Scan Activity Bar 18
6.3.1. Scan Files and Folders 19
6.3.2. Disable/Restore Scan Activity Bar 19
6.4. Automatic Device Detection 20

7. Main Application Window 22
7.1. Basic View 23
7.1.1. Status Area 23
7.1.2. Protect Your PC Area 24
7.2. Intermediate View 24
7.2.1. Dashboard 25
7.2.2. Security 26
7.2.3. Network 27
7.3. Expert View 27

8. My Tools 29

9. Alerts and Pop-ups 32
9.1. Antivirus Alerts 32
9.2. Active Virus Control Alerts 33
9.3. Device Detection Alerts 33
9.4. Antiphishing Alerts 34
9.5. Privacy Control Alerts 35
9.5.1. Registry Alerts 35
9.5.2. Script Alerts 36
9.5.3. Cookie Alerts 36
10. Fixing Issues 37
10.1. Fix Issues Wizard 37
10.2. Configuring Status Alerts 38
11. Configuring Main Settings 40
11.1. Security Settings 40
11.2. Alerts Settings 42
11.3. General Settings 42
11.4. Reconfiguring the Usage Profile 43
12. History and Events 45
13. Registration 46
13.1. Registering SHIELD DELUXE 2013 46
13.2. Buying or Renewing License Keys 46
Configuration and Management 48
14. General Settings 49
15. Antivirus Protection 54
15.1. Real-time Protection 54
15.1.1. Adjusting the Real-time Protection Level 55
15.1.2. Creating a Custom Protection Level 56
15.1.3. Changing the Actions Taken on Detected Files 57
15.1.4. Restoring the Default Settings 59
15.1.5. Configuring Active Virus Control 59
15.1.6. Configuring the Intrusion Detection System 61
15.2. On-demand Scanning 62
15.2.1. Scanning Files and Folders 62
15.2.2. Antivirus Scan Wizard 64
15.2.3. Viewing Scan Logs 67
15.2.4. Managing Existing Scan Tasks 67
15.3. Configuring Scan Exclusions 74
15.3.1. Excluding Files or Folders from Scanning 75
15.3.2. Excluding File Extensions from Scanning 76
15.3.3. Managing Scan Exclusions 77

15.4. Quarantine Area 78

16. Antiphishing Protection 80
16.1. Configuring the Antiphishing White List 80
16.2. Managing the SHIELD DELUXE Antiphishing Protection in Internet Explorer and Firefox 81

17. Search Advisor 83
17.1. Disabling Search Advisor 83

18. Privacy Control 84
18.1. Configuring Protection Level 84
18.2. Identity Control 85
18.2.1. About Identity Control 85
18.2.2. Configuring Identity Control 86
18.2.3. Managing Rules 89
18.3. Registry Control 89
18.4. Cookie Control 90
18.5. Script Control 92

19. Vulnerability 94
19.1. Checking for Vulnerabilities 94
19.2. Status 95
19.3. Settings 96

20. Chat Encryption 97
20.1. Disabling Encryption for Specific Users 98
20.2. SHIELD DELUXE Toolbar in the Chat Window 98

21. Game / Laptop Mode 99
21.1. Game Mode 99
21.1.1. Configuring Automatic Game Mode 100
21.1.2. Managing the Game List 100
21.1.3. Adding or Editing Games 101
21.1.4. Configuring Game Mode Settings 101
21.1.5. Changing Game Mode Hotkey 101
21.2. Laptop Mode 102
21.2.1. Configuring Laptop Mode Settings 102
21.3. Silent Mode 103
21.3.1. Configuring Full Screen Action 103
21.3.2. Configuring Silent Mode Settings 104

22. Home Network 105
22.1. Enabling the SHIELD DELUXE Network 105
22.2. Adding Computers to the SHIELD DELUXE Network 106
22.3. Managing the SHIELD DELUXE Network 107

23. Update 109

23.1. Performing an Update 109
23.2. Configuring Update Settings 110
23.2.1. Setting Update Locations 111
23.2.2. Configuring Automatic Update 111
23.2.3. Configuring Manual Update 112
23.2.4. Configuring Advanced Settings 112

How To *113*

24. How Do I Scan Files and Folders? 114
24.1. Using Windows Contextual Menu 114
24.2. Using Scan Tasks 114
24.3. Using Scan Activity Bar 116

25. How Do I Create a Custom Scan Task? 117

26. How Do I Schedule a Computer Scan? 119

27. How Do I Update SHIELD DELUXE Using a Proxy Server? . 121

Troubleshooting and Getting Help *122*

28. Troubleshooting 123
28.1. Installation Problems 123
28.1.1. Installation Validation Errors 123
28.1.2. Failed Installation 124
28.2. My System Appears to Be Slow 125
28.3. Scan Doesn't Start 126
28.4. I Can no Longer Use an Application 126
28.5. How to Update SHIELD DELUXE on a Slow Internet Connection 127
28.6. SHIELD DELUXE Services Are Not Responding 128
28.7. SHIELD DELUXE Removal Failed 129

29. Removing Malware from Your System 130
29.1. What to Do When SHIELD DELUXE Finds Viruses on Your Computer? 130
29.2. How Do I Clean a Virus in an Archive? 131
29.3. How Do I Clean a Virus in an E-Mail Archive? 132
29.4. What to Do When SHIELD DELUXE Detected a Clean File as Infected? . . . 133
29.5. How to Clean the Infected Files from System Volume Information 133
29.6. What Are the Password-Protected Files in the Scan Log? 135
29.7. What Are the Skipped Items in the Scan Log? 135
29.8. What Are the Over-Compressed Files in the Scan Log? 135
29.9. Why Did SHIELD DELUXE Automatically Delete an Infected File? 136

30. Support 137

31. Useful Information 138

31.1. How Do I Remove Other Security Solutions? 138
31.2. How Do I Restart in Safe Mode? 139
31.3. Am I Using a 32 bit or a 64 bit Version of Windows? 139
31.4. How Do I Find Out My Proxy Settings? 140
31.5. How Do I Remove SHIELD DELUXE Completely? 140
31.6. How Do I Enable / Disable the Real Time Protection? 141
31.7. How Do I Display Hidden Objects in Windows? 142

Glossary 143

Installation and Removal

1. System Requirements

You may install SHIELD DELUXE 2013 only on computers running the following operating systems:

- Windows XP with Service Pack 3 (32 bit)
- Windows Vista with Service Pack 2
- Windows 7 with Service Pack 1
- Windows 8

Before installation, make sure that your computer meets the minimum hardware and software requirements.

Note

To find out the Windows operating system your computer is running and hardware information, right-click **My Computer** on the desktop and then select **Properties** from the menu.

1.1. Minimal System Requirements

- 1.8 GB available free hard disk space (at least 800 MB on the system drive)
- 800 MHz processor
- RAM Memory:
  - 1 GB

1.2. Recommended System Requirements

- 2.8 GB available free hard disk space (at least 800 MB on the system drive)
- Intel CORE Duo (1.66 GHz) or equivalent processor
- RAM Memory:
  - 1 GB for Windows XP
  - 1.5 GB for Windows Vista, Windows 7 and Windows 8

1.3. Software Requirements

- Internet Explorer 7.0 or higher
- .NET Framework 3.5 (automatically installed by PCSecurityShield if necessary)
- Mozilla Firefox 3.6 or higher
- Thunderbird 3.0.4
- Outlook 2007, 2010
- Outlook Express and Windows Mail on x86

2. Preparing for Installation

Before you install SHIELD DELUXE 2013, complete these preparations to ensure the installation will go smoothly:

- Make sure that the computer where you plan to install SHIELD DELUXE 2013 meets the minimum system requirements. If the computer does not meet all the minimum system requirements, SHIELD DELUXE 2013 will not be installed or, if installed, it will not work properly and it will cause system slowdowns and instability. For a complete list of system requirements, please refer to "*System Requirements*" (p. 2).
- Log on to the computer using an Administrator account.
- Remove any other security software from the computer. Running two security programs simultaneously may affect their operation and cause major problems with the system. Windows Defender will be disabled by default before installation is initiated.

3. Installing SHIELD DELUXE 2013

You can purchase SHIELD DELUXE 2013 and download the installation file from the PCSecurityShield website at http://www.PCSecurityShield.com/.

To install SHIELD DELUXE 2013, locate the installation file on your computer and double-click it. This will launch a wizard, which will guide you through the installation process.

The installer will first check your system to validate the installation. If the installation is validated, the setup wizard will appear.

The wizard will help you install SHIELD DELUXE on your computer and at the same time will allow you to configure the main settings and user interface.

3.1. Step 1 - Introduction

Please read the License Agreement and select **By checking this box, I agree to the SHIELD DELUXE license agreement**. Click **Next** to continue.

If you do not agree to these terms click **Cancel**. The installation process will be abandoned and you will exit setup.

3.2. Step 2 - Preparing Install

SHIELD DELUXE scans your system and checks if any other security software is installed on it.

Quick Scan

A quick scan of critical areas on your system is performed to ensure no active malware is residing on it.

The scan shouldn't take more than a few minutes. You can cancel it at any time by using the provided button.

Important

It is highly recommended to allow the scan to complete. Active malware could disrupt the installation and even cause it to fail.

After the scan is completed, the results are displayed. If any threats are detected, follow the instructions to remove them before continuing the installation.

Click **Next** to continue.

Removing Existing Security Software

SHIELD DELUXE 2013 alerts you if you have other security products installed on your computer. Click the corresponding button to start the uninstall process and follow the instructions to remove any detected products.

> *Warning*
> It is highly recommended that you uninstall any other antivirus products detected before installing SHIELD DELUXE. Running two or more antivirus products at the same time on a computer usually renders the system unusable.

If Windows Defender is enabled, it is also recommended to allow SHIELD DELUXE to turn it off.

Click **Next** to continue.

3.3. Step 3 - Registration

SHIELD DELUXE registration process consists in registering your product with a license key.

Register Your Product

SHIELD DELUXE 2013 comes with 14-day trial period. During the trial period, the product is fully functional and you can test it to see if it meets your expectations. To begin the trial period, select **I want to evaluate SHIELD DELUXE 2013 for 14 days** and click **Next**.

If you have already purchased SHIELD DELUXE 2013, follow these steps to register your product:

1. Select **I want to register SHIELD DELUXE with a license key**.
2. Type the license key in the edit field.

> *Note*
> You can find your license key:
> ■ on the "Thank You" page after your order.

- in your order confirmation e-mail.
- at the PCSecurityShield customer center.

If you do not have a license key for SHIELD DELUXE 2013, click the provided link to go to the online store and buy one.

3. Click **Register Now**.
4. Click **Next**.

3.4. Step 4 - Choose View

This is where you choose the type of installation to perform and the interface view mode to use.

Choose Setup Type

The following setup options are available:

- **Easy Setup** - select this option if you prefer a quick installation and do not intend to configure SHIELD DELUXE settings in detail.
- **Custom Setup** - select this option if you prefer to customize the installation and the SHIELD DELUXE settings.

To see a video tutorial that will help you with the installation, click **Get Help**

Note
To install SHIELD DELUXE in a default configuration and go straight to the last step of the installation wizard, select **Skip Setup**.

Click **Next** to continue.

Choose Setup Location

Note
This step appears only if you have chosen a **Custom Setup**.

By default, SHIELD DELUXE 2013 will be installed in `C:\Program Files\SHIELD DELUXE\`. If you want to change the installation path, click **Browse** and select the folder in which you would like SHIELD DELUXE to be installed.

You can share the product files and signatures with other SHIELD DELUXE users. This way, SHIELD DELUXE updates can be performed faster. If you don't want to enable this feature, select the corresponding check box.

Note
No personal identifiable information will be shared if this feature is enabled.

Click **Next** to continue.

Choose User Interface

Select the user interface view mode that best suits your needs. SHIELD DELUXE 2013 gives you a choice of three interfaces, each tailored to the needs of a different type of user.

Basic View

Suited for computer beginners and people who want SHIELD DELUXE to protect their computer and data without being bothered. The interface is simple to use and requires minimal interaction on your side.

All you have to do is fix the existing issues when indicated by SHIELD DELUXE. An intuitive step-by-step wizard assists you in fixing issues. Additionally, you can perform common tasks, such as updating the SHIELD DELUXE virus signature and product files or scanning the computer.

Intermediate View

You can configure the main SHIELD DELUXE settings, fix issues separately, manage the SHIELD DELUXE products installed on the computers in your household and choose which issues to be monitored.

Expert View

Suited for more technical users, this mode allows you to fully configure each functionality of SHIELD DELUXE. You can also use all tasks provided to protect your computer and data.

Make your selection and click **Next** to continue.

3.5. Step 5 - Configure

This is where you can customize your product.

Configure Settings

Note
This step appears only if you have set the SHIELD DELUXE interface to **Expert View**.

Here you can enable / disable SHIELD DELUXE features organized in two categories. To change the status of a setting, click the corresponding switch.

- **Security Settings**

  In this area, you can enable or disable product settings that cover various aspects of computer and data security.

Setting	*Description*
Antivirus	Real-time protection ensures that all files are scanned as they are accessed by you or by an application running on this system.
Automatic Update	Automatic update ensures that the newest SHIELD DELUXE product and signature files are downloaded and installed automatically, on a regular basis.
Vulnerability Check	Automatic vulnerability check ensures that crucial software on your PC is up-to-date.
Antiphishing	Antiphishing detects and alerts you in real-time if a web page is set up to steal personal information.
Identity Control	Identity Control helps you prevent your personal data from being sent out on the Internet without your consent. It blocks any instant messages, e-mail messages or web forms transmitting data you defined as being private to unauthorized recipients (addresses).
Chat Encryption	Chat Encryption secures your conversations via Yahoo! Messenger and Windows Live Messenger provided that your IM contacts use a compatible SHIELD DELUXE product and IM software.

- **General Settings**

In this area, you can enable or disable settings that affect product behavior and user experience.

Setting	*Description*
Game Mode	Game Mode temporarily modifies protection settings so as to minimize their impact on system performance during games.
Laptop Mode Detection	Laptop Mode temporarily modifies protection settings so as to minimize their impact on the life of your laptop battery.
Settings Password	This ensures that the SHIELD DELUXE settings can only be changed by the person who knows this password. When you enable this option, you will be prompted to configure the settings password. Type the desired password in both fields and click **OK** to set the password.
SHIELD DELUXE News	By enabling this option, you will receive important company news, product updates or new security threats from SHIELD DELUXE.
Product Notification Alerts	By enabling this option, you will receive information alerts.
Scan Activity Bar	The Scan Activity Bar is a small, transparent window indicating the progress of the SHIELD DELUXE scanning activity. For more information, please refer to "*Scan Activity Bar*" (p. 18).
Send Virus Reports	By enabling this option, virus scanning reports are sent to SHIELD DELUXE labs for analysis. Please note that these reports will contain no confidential data, such as your name or IP address, and that they will not be used for commercial purposes.
Outbreak Detection	By enabling this option, reports regarding potential virus-outbreaks are sent to SHIELD DELUXE labs for analysis. Please note that these reports will contain no confidential data, such as your name or IP address,

Setting	Description
	and that they will not be used for commercial purposes.

Click **Next** to continue.

Configure My Tools

Note
This step appears only if you have set the SHIELD DELUXE interface to **Basic View** or **Intermediate View**.

With **My Tools**, you can personalize the dashboard by adding shortcuts to the tools that are most important to you. This way you can ensure easy access to them.

From this screen, you can add shortcuts for any of the following tools:

- Game Mode - set up SHIELD DELUXE so as not to allow it to interfere with your gaming experience.
- Laptop Mode - temporarily modifies protection settings so as to minimize their impact on the life of your laptop battery.
- Home Network Management - manage SHIELD DELUXE products installed on computers in the home network from a single PC.
- Full System Scan - perform a scan of the entire system.

Select the tools you want to add and click **Next** to continue.

Home Network Management

Note
This step appears only if you have added Home Network Management to My Tools.

You can select one of three options:

- **Set up this PC as Server**

  Select this option if you intend to manage SHIELD DELUXE products on other computers in the home network from this one.

A password is required to join the network. Enter the password in the provided text boxes and click **Submit**.

- **Set up this PC as Client**

  Select this option if SHIELD DELUXE will be managed from another computer in the home network which is also running SHIELD DELUXE.

  A password is required to join the network. Enter the password in the provided text boxes and click **Submit**.

- **Skip setup for now**

  Select this option to configure this feature at a later time from the SHIELD DELUXE window.

Click **Next** to continue.

3.6. Step 6 - Support Options

Enable / disable **Smart Tips**. Smart Tips are personalized messages displayed in the SHIELD DELUXE Dashboard to help you improve your computer's performance.

3.7. Step 7 - Confirm

This is where you can review the selected configuration.

By default, two tasks are also scheduled:

- A full system scan is scheduled immediately after the installation is finished.

  It is recommended to perform this thorough scan that will detect any malware threats present on your system.

- A system scan is scheduled for every Sunday at 2 AM.

  It is highly recommended to scan your system at least once a week. Select a different day and time if the default schedule is not suitable for you. If the computer is shut down when the schedule is due, the scan will run the next time you start your computer.

Click **Finish**.

3.8. Step 8 - Finish

The installation is now nearing completion. The final settings are applied and an update is performed.

The wizard will automatically close when the installation is completed. If this option was selected during the previous step, a full system scan is initiated.

Note

A system restart may be required.

4. Upgrade

In order to upgrade an older version of SHIELD DELUXE to SHIELD DELUXE 2013, follow these steps:

1. Remove the older version of SHIELD DELUXE from your computer. For more information, please refer to the help file or user manual of the product.
2. Restart the computer.
3. Install SHIELD DELUXE 2013 as described in the "*Installing SHIELD DELUXE 2013*" (p. 5) section of this user guide.

5. Repairing or Removing SHIELD DELUXE

If you want to repair or remove SHIELD DELUXE 2013, follow the path from the Windows start menu: **Start** → **All Programs** → **SHIELD DELUXE 2013** → **Repair or Remove**.

A wizard will appear to help you complete the desired task.

1. **Repair or Remove**

   Select the action you want to perform:

   - **Repair** - to re-install all program components.
   - **Remove** - to remove all installed components.

   Note
   We recommend that you choose **Remove** for a clean re-installation.

2. **Confirm Action**

   Make sure to read the information displayed carefully before clicking **Next** to confirm the action.

3. **Progress**

   Wait for SHIELD DELUXE 2013 to complete the action you have selected. This will take several minutes.

4. **Finish**

   The results are displayed.

   You need to restart the computer to complete the process. Click **Restart** to reboot your computer immediately, or **Finish** to close the window and reboot at a later time.

Getting Started

6. Overview

Once you have installed SHIELD DELUXE 2013, your computer is protected against all kinds of malware (such as viruses, spyware and trojans).

You are not required to configure other SHIELD DELUXE 2013 settings besides those configured during installation. However, you may want to take advantage of SHIELD DELUXE 2013 settings to fine-tune and improve your protection.

From time to time, you should open SHIELD DELUXE 2013 and fix the existing issues. You may have to configure specific SHIELD DELUXE 2013 components or take preventive actions to protect your computer and your data. If you want to, you can configure SHIELD DELUXE 2013 not to alert you about specific issues.

If you have not registered the product during installation, remember to do so until the trial period ends. For more information on the registration process, please refer to “*Registration*” (p. 46).

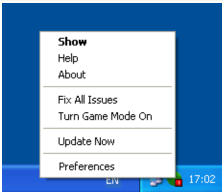
6.1. Opening SHIELD DELUXE 2013

To access the main interface of SHIELD DELUXE 2013, use the Windows Start menu, by following the path **Start** → **All Programs** → **SHIELD DELUXE 2013** → **SHIELD DELUXE 2013** or, quicker, double-click SHIELD DELUXE 2013 icon ● in the system tray.

For more information on the main application window, please refer to “*Main Application Window*” (p. 22).

6.2. System Tray Icon

To manage the entire product more quickly, you can use SHIELD DELUXE 2013 icon ● in the system tray. If you double-click this icon, SHIELD DELUXE 2013 will open. Also, by right-clicking the icon, a contextual menu will allow you to quickly manage SHIELD DELUXE 2013 product.



Tray Icon

- **Show** - opens the main interface of SHIELD DELUXE 2013.
- **Help** - opens the help file, which explains in detail how to configure and use SHIELD DELUXE 2013.
- **About** - opens a window where you can see information about SHIELD DELUXE 2013 and where to look for help in case something unexpected appears.
- **Fix All Issues** - helps you remove current security vulnerabilities. If the option is unavailable, there are no issues to be fixed. For detailed information, please refer to "*Fixing Issues*" (p. 37).
- **Turn Game Mode On / Off** - activates / deactivates Game Mode.
- **Update Now** - starts an immediate update. A new window will appear where you can see the update status.
- **Preferences** - opens a window where you can enable or disable the main product settings and reconfigure your user profile. For more information, please refer to "*Configuring Main Settings*" (p. 40).

SHIELD DELUXE 2013 system tray icon informs you when issues affect your computer or how the product operates, by displaying a special symbol, as follows:

Red square with an exclamation mark: Critical issues affect the security of your system. They require your immediate attention and must be fixed as soon as possible.
Yellow square with an exclamation mark: Non-critical issues affect the security of your system. You should check and fix them when you have the time.
Letter G: The product operates in Game Mode.

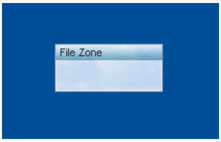
If SHIELD DELUXE 2013 is not working, the system tray icon is grayed out . This usually happens when the license key expires. It can also occur when SHIELD DELUXE 2013 services are not responding or when other errors affect the normal operation of SHIELD DELUXE 2013.

6.3. Scan Activity Bar

The **Scan activity bar** is a graphic visualization of the scanning activity on your system. This small window is by default available only in Expert View.

The gray bars (the **File Zone**) show the number of scanned files per second, on a scale from 0 to 50.

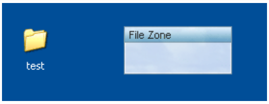
Note
The Scan activity bar will notify you when real-time protection is disabled by displaying a red cross over the **File Zone**.



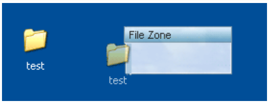
Scan Activity Bar

6.3.1. Scan Files and Folders

You can use the Scan activity bar to quickly scan files and folders. Drag the file or folder you want to be scanned and drop it over the **Scan Activity Bar** as shown below.



Drag File



Drop File

The Antivirus Scan wizard will appear and guide you through the scanning process.

Scanning options. The scanning options are pre-configured for the best detection results. If infected files are detected, SHIELD DELUXE 2013 will try to disinfect them (remove the malware code). If disinfection fails, the Antivirus Scan wizard will allow you to specify other actions to be taken on infected files. The scanning options are standard and you cannot change them.

6.3.2. Disable/Restore Scan Activity Bar

When you no longer want to see the graphic visualization, just right-click it and select **Hide**. To restore the Scan activity bar, follow these steps:

1. Open SHIELD DELUXE 2013.

2. Click the **Options** button in the upper-right corner of the window and select **Preferences**.
3. In the General Settings category, use the switch corresponding to **Scan Activity Bar** to enable it.
4. Click **OK** to save and apply the changes.

6.4. Automatic Device Detection

SHIELD DELUXE 2013 automatically detects when you connect a removable storage device to your computer and offers to scan it before you access its files. This is recommended in order to prevent viruses and other malware from infecting your computer.

Detected devices fall into one of these categories:

- CDs/DVDs
- USB storage devices, such as flash pens and external hard-drives
- mapped (remote) network drives

When such a device is detected, an alert window is displayed.

To scan the storage device, just click **Yes**. The Antivirus Scan wizard will appear and guide you through the scanning process.

If you do not want to scan the device, you must click **No**. In this case, you may find one of these options useful:

- **Don't ask me again about this type of device** - SHIELD DELUXE 2013 will no longer offer to scan storage devices of this type when they are connected to your computer.
- **Disable automatic device detection** - You will no longer be prompted to scan new storage devices when they are connected to the computer.

If you accidentally disabled automatic device detection and you want to enable it, or if you want to configure its settings, follow these steps:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus>Virus Scan**.
3. In the list of scan tasks, locate the **Device Scanning** task.
4. Right-click the task and select **Properties**. A new window will appear.

5. On the **Overview** tab, configure the scanning options as needed. For more information, please refer to "*Configuring Scan Settings*" (p. 70).
6. On the **Detection** tab, choose which types of storage devices to be detected.
7. Click **OK** to save and apply the changes.

7. Main Application Window

SHIELD DELUXE 2013 meets the needs of computer beginners and very technical people alike. Its graphical user interface is designed to suit each and every category of users.

You can choose to view the user interface under any of three modes, depending on your computer skills and on your previous experience with SHIELD DELUXE 2013.

Basic View

Suited for computer beginners and people who want SHIELD DELUXE 2013 to protect their computer and data without being bothered. This mode is simple to use and requires minimal interaction on your side.

All you have to do is fix the existing issues when indicated by SHIELD DELUXE 2013. An intuitive step-by-step wizard assists you in fixing issues. Additionally, you can perform common tasks, such as updating SHIELD DELUXE 2013 virus signature and product files or scanning the computer.

Intermediate View

Aimed at users with average computer skills, this interface extends what you can do in Basic View.

You can fix issues separately and choose which issues to be monitored. Moreover, you can manage remotely SHIELD DELUXE 2013 products installed on the computers in your household.

Expert View

Suited for more technical users, this mode allows you to fully configure each functionality of SHIELD DELUXE 2013. You can also use all tasks provided to protect your computer and data.

The view mode is selected during installation.

To change the view mode:

1. Open SHIELD DELUXE 2013.
2. Click the **Options** button in the upper-right corner of the window.
3. Select the desired view mode from the menu.

7.1. Basic View

If you are a computer beginner, displaying the user interface in Basic View may be the most adequate choice for you. This mode is simple to use and requires minimal interaction on your side.

The window is organized into three main areas:

Status area
: Status information is presented in the left side of the window.

Protect Your PC area
: This is where you can take the necessary actions to manage your protection.

Smart Tips area
: **Smart Tips** are a fun and easy way to learn about computer security best practices and how to use SHIELD DELUXE 2013.

The **Options** button in the upper-right corner of the window allows you to change the user interface view mode and to configure the main program settings.

In the bottom-right corner of the window, you can find several useful links.

Link	*Description*
License Info	Opens a window where you can see current license key information and register your product with a new license key.
View Logs	Allows you to see a detailed history of all tasks performed by SHIELD DELUXE 2013 on your system.
Help and Support	Click this link if you need help with SHIELD DELUXE 2013.
?	Gives you access to a help file that shows you how to use The Shield Deluxe.

7.1.1. Status Area

Status information is presented in the left side of the window.

- **Security Status** informs you of the issues that affect your computer's security and helps you fix them. By clicking **Fix All Issues**, a wizard will help you easily remove any threats to your computer and data security. For detailed information, please refer to "*Fixing Issues*" (p. 37).

- **License Status** displays how many days are left until the license expires. If you are using a trial version or if your license is going to expire, you can click **Buy Now** to buy a license key. For detailed information, please refer to "*Registration*" (p. 46).

7.1.2. Protect Your PC Area

This is where you can take the necessary actions to manage your protection.

Three buttons are available:

- **Security** provides you with shortcuts to security tasks and settings.
- **Update Now** helps you update the virus signature and product files of SHIELD DELUXE 2013. A new window will appear where you can see the update status. If updates are detected, they are automatically downloaded and installed on your computer.
- **My Tools** allows you to create shortcuts to your favorite tasks and settings.

To perform a task or configure settings, click the corresponding button and choose the desired tool from the menu. To add or remove shortcuts, click the corresponding button and choose **More Options**. For detailed information, please refer to "*My Tools*" (p. 29).

7.2. Intermediate View

Aimed at users with average computer skills, Intermediate View is a simple interface that gives you access to all modules at a basic level. You'll have to keep track of warnings and critical alerts and fix undesired issues.

The Intermediate View window is organized into several tabs.

Dashboard

The dashboard helps you easily monitor and manage your protection.

Security

Displays the status of the security settings and helps you fix detected issues. You can run security tasks or configure security settings.

Network

Displays SHIELD DELUXE 2013 home network structure. This is where you can perform various actions to configure and manage SHIELD DELUXE 2013 products installed in your home network. In this way, you can manage the security of your home network from a single computer.

The **Options** button in the upper-right corner of the window allows you to change the user interface view mode and to configure the main program settings.

In the bottom-right corner of the window, you can find several useful links.

Link	*Description*
License Info	Opens a window where you can see current license key information and register your product with a new license key.
View Logs	Allows you to see a detailed history of all tasks performed by SHIELD DELUXE 2013 on your system.
Buy/Renew 2013	Helps you purchase a license key for your SHIELD DELUXE 2013 product.
Help and Support	Click this link if you need help with SHIELD DELUXE 2013.
?	Gives you access to a help file that shows you how to use The Shield Deluxe.

7.2.1. Dashboard

The dashboard helps you easily monitor and manage your protection.

The dashboard consists of the following sections:

- **Status Details** indicates the status of each main module using explicit sentences and one of the following icons:

  ✓ **Green circle with a check mark:** No issues affect the security status. Your computer and data are protected.

  ❗ **Red circle with an exclamation mark:** There are issues that affect the security of your system. Critical issues require your immediate attention. Non-critical issues should also be addressed as soon as possible.

  ⊗ **Gray circle with an exclamation mark:** The activity of this module's components is not monitored. Thus, no information is available regarding their security status. There may be specific issues related to this module.

  Click the name of a module to see more details about its status and to configure status tracking for its components.

- **License Status** displays how many days are left until the license expires. If you are using a trial version or if your license is going to expire, you can click **Buy Now** to buy a license key. For detailed information, please refer to "*Registration*" (p. 46).

- **My Tools** allows you to create shortcuts to your favorite tasks and settings. For detailed information, please refer to "*My Tools*" (p. 29).
- **Smart Tips** are a fun and easy way to learn about computer security best practices and how to use SHIELD DELUXE 2013.

7.2.2. Security

The Security tab allows you to manage the security of your computer and data.

"Status Area" (p. 26)
"Quick Tasks" (p. 26)

Status Area

The status area is where you can see the complete list of monitored security components and their current status. By monitoring each security module, SHIELD DELUXE 2013 will let you know not only when you configure settings that might affect your computer's security, but also when you forget to do important tasks.

The current status of a component is indicated using explicit sentences and one of the following icons:

✅ **Green circle with a check mark:** No issues affect the component.

❗ **Red circle with an exclamation mark:** Issues affect the component.

Just click the **Fix** button corresponding to a sentence to fix the reported issue. If an issue is not fixed on the spot, follow the wizard to fix it.

To configure which components must be monitored:

1. Click **Add/Edit List**.
2. To turn on or off monitoring for a specific item, use the corresponding switch.
3. Click **Close** to save the changes and close the window.

Important
To ensure that your system is fully protected, enable tracking for all components and fix all reported issues.

Quick Tasks

This is where you can find links to the most important security tasks:

- **Update Now** - starts an immediate update.

- **Full System Scan** - starts a standard scan of your computer (archives excluded). For additional on-demand scan tasks, click the arrow ▾ on this button and select a different scan task.
- **Custom Scan** - starts a wizard that lets you create and run a custom scan task.
- **Vulnerability Scan** - starts a wizard that checks your system for vulnerabilities and helps you fix them.

7.2.3. Network

This is where you can perform various actions to configure and manage SHIELD DELUXE 2013 products installed in your home network. In this way, you can manage the security of your home network from a single computer.

For detailed information, please refer to "*Home Network*" (p. 105).

7.3. Expert View

Expert View gives you access to each specific component of SHIELD DELUXE 2013. This is where you can configure SHIELD DELUXE 2013 in detail.

Note
Expert View is suited for users having above average computer skills, who know the type of threats a computer is exposed to and how security programs work.

On the left side of the window there is a menu containing all security modules. Each module has one or more tabs where you can configure the corresponding security settings or perform security or administrative tasks. The following list briefly describes each module. For detailed information, please refer to the "Configuration and Management" (p. 48) part of this user guide.

General
: Allows you to access the general settings or to view the dashboard and detailed system info.

Antivirus
: Allows you to configure your virus shield and scanning operations in detail, to set exceptions and to configure the quarantine module. This is were you can also configure antiphishing protection and Search Advisor.

Privacy Control

Allows you to prevent data theft from your computer and protect your privacy while you are online.

Vulnerability

Allows you to keep crucial software on your PC up-to-date.

Encryption

Allows you to encrypt Yahoo and Windows Live (MSN) Messenger communications.

Game/Laptop Mode

Allows you to postpone SHIELD DELUXE 2013 scheduled tasks while your laptop runs on batteries and also to eliminate all alerts and pop-ups when you are playing.

Home Network

Allows you to configure and manage several computers in your household.

Update

Allows you to obtain info on the latest updates, to update the product and to configure the update process in detail.

Registration

Displays your registration information and allows you to register SHIELD DELUXE 2013 2013 with a license key.

The **Options** button in the upper-right corner of the window allows you to change the user interface view mode and to configure the main program settings.

In the bottom-right corner of the window, you can find several useful links.

Link	*Description*
License Info	Opens a window where you can see current license key information and register your product with a new license key.
View Logs	Allows you to see a detailed history of all tasks performed by SHIELD DELUXE 2013 on your system.
Buy/Renew 2013	Helps you purchase a license key for your SHIELD DELUXE 2013 product.
Help and Support	Click this link if you need help with SHIELD DELUXE 2013. Gives you access to a help file that shows you how to use The Shield Deluxe.

8. My Tools

When using SHIELD DELUXE 2013 in Basic View or Intermediate View, you can customize your dashboard by adding shortcuts to tasks and settings that are important to you. This way, you can quickly gain access to features you use regularly and to advanced settings without having to switch to a more advanced interface view mode.

Depending on the user interface view mode you use, the shortcuts added to My Tools are available as follows:

Basic View

In the Protect Your PC area, click My Tools. A menu will appear. Click a shortcut to launch the corresponding tool.

Intermediate View

The shortcuts appear under My Tools. Click a shortcut to launch the corresponding tool.

To open the window from which you can select the shortcuts that will appear in My Tools, proceed as follows:

Basic View

In the Protect Your PC area, click My Tools and choose **More Options**.

Intermediate View

Click one of the buttons under My Tools or the **Configure** link.

Use the switches to select the tools to be added to My Tools. You can select any of the following categories of tools.

- **Scan Tasks**

  Add the tasks you regularly use to scan your system for security threats.

Scan Task	*Description*
Deep System Scan	Scans the entire system. In the default configuration, it scans for all types of malware threatening your system's security, such as viruses, spyware, adware, rootkits and others.

Scan Task	*Description*
Full System Scan	Scans the entire system, except for archives. In the default configuration, it scans for all types of malware other than rootkits.
Quick Scan	Quick Scan uses in-the-cloud scanning to detect malware running in your system. Running a Quick Scan usually takes less than a minute and uses a fraction of the system resources needed by a regular virus scan.
Custom Scan	Starts a wizard that lets you create a custom scan task.
My Documents Scan	Use this task to scan important current user folders: `My Documents`, `Desktop` and `StartUp`. This will ensure the safety of your documents, a safe workspace and clean applications running at startup.
Schedule My Scans	Takes you to the Antivirus settings window where you can customize the on-demand scan tasks.

For more information about scan tasks, please refer to "*Managing Existing Scan Tasks*" (p. 67).

- **Settings**

  Add shortcuts to SHIELD DELUXE 2013 settings you want to configure:

Settings	*Description*
Configure Antivirus	Configure the Antivirus module. For more information, please refer to "*Antivirus Protection*" (p. 54).
Game Mode	Toggle the Game Mode. For more information, please refer to "*Game Mode*" (p. 99).
Laptop Mode	Toggle the Laptop Mode. For more information, please refer to "*Laptop Mode*" (p. 102).
Update Now	Trigger an update of SHIELD DELUXE 2013. For more information, please refer to "*Update*" (p. 109).

Settings	*Description*
View & Fix All Issues	Open a wizard that will help you fix all the security issues affecting your system. For more information, please refer to "*Fixing Issues*" (p. 37).

- **Help & Support**

  Allows you to contact the PCSecurityShield support team.

9. Alerts and Pop-ups

SHIELD DELUXE 2013 uses pop-ups and alerts to inform you about its operation or special events that may interest you and to prompt you for action when needed. This chapter presents SHIELD DELUXE 2013 pop-ups and alerts that you may encounter.

Pop-ups are small windows that temporarily appear on the screen to inform you about various SHIELD DELUXE 2013 events, such as e-mail scanning, a new computer that logged to your wireless network, a firewall rule added etc. When pop-ups appear, you will be required to click an **OK** button or a link, at the most.

Alerts are larger windows that prompt you for action or inform you about something very important (for example, a virus has been detected). Besides alert windows, you may receive e-mail, instant message or web page alerts.

SHIELD DELUXE 2013 pop-ups and alerts include:

- Antivirus Alerts
- Active Virus Control Alerts
- Device Detection Alerts
- Antiphishing Alert Web Pages
- Privacy Control Alerts

9.1. Antivirus Alerts

SHIELD DELUXE 2013 protects you against various kinds of malware, such as viruses, spyware or rootkits. When it detects a virus or other malware, SHIELD DELUXE 2013 takes a specific action on the infected file and informs you about it through an alert window.

You can see the virus name, the path to the infected file and the action taken by The Shield Deluxe.

Click **OK** to close the window.

Important

When a virus is detected, it is best practice to scan the entire computer to make sure there are no other viruses. For more information, please refer to "*How Do I Scan Files and Folders?*" (p. 114).
If the virus has not been blocked, please refer to "*Removing Malware from Your System*" (p. 130).

9.2. Active Virus Control Alerts

Active Virus Control can be configured to alert you and prompt you for action whenever an application tries to perform a possible malicious action.

If you are using the Basic View or Intermediate View interface, a pop-up will inform you whenever Active Virus Control blocks a potentially harmful application. If you are using Expert View, you will be prompted for action, through an alert window, when an application exhibits malicious behavior.

If you know and trust the detected application, click **Allow**.

If you want to immediately close the application, click **OK**.

Select the **Remember this action for this application** check box before making your choice and SHIELD DELUXE 2013 will take the same action for the detected application in the future. The rule that is thus created will be listed in the Active Virus Control configuration window.

9.3. Device Detection Alerts

SHIELD DELUXE 2013 automatically detects when you connect a removable storage device to your computer and offers to scan it before you access its files. This is recommended in order to prevent viruses and other malware from infecting your computer.

Detected devices fall into one of these categories:

- CDs/DVDs
- USB storage devices, such as flash pens and external hard-drives
- mapped (remote) network drives

When such a device is detected, an alert window is displayed.

To scan the storage device, just click **Yes**. The Antivirus Scan wizard will appear and guide you through the scanning process.

If you do not want to scan the device, you must click **No**. In this case, you may find one of these options useful:

- **Don't ask me again about this type of device** - SHIELD DELUXE 2013 will no longer offer to scan storage devices of this type when they are connected to your computer.
- **Disable automatic device detection** - You will no longer be prompted to scan new storage devices when they are connected to the computer.

If you accidentally disabled automatic device detection and you want to enable it, or if you want to configure its settings, follow these steps:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus>Virus Scan**.
3. In the list of scan tasks, locate the **Device Scanning** task.
4. Right-click the task and select **Properties**. A new window will appear.
5. On the **Overview** tab, configure the scanning options as needed. For more information, please refer to "*Configuring Scan Settings*" (p. 70).
6. On the **Detection** tab, choose which types of storage devices to be detected.
7. Click **OK** to save and apply the changes.

9.4. Antiphishing Alerts

With antiphishing protection enabled, SHIELD DELUXE 2013 alerts you when you try to access web pages that may be set up to steal personal information. Before you can access such a web page, SHIELD DELUXE 2013 will block that page and display a generic web page alert instead.

Check the web page address in the address bar of your browser. Look for clues that might indicate that the web page is used for phishing. If the web address is suspicious, it is recommended that you do not open it.

Here are some tips you may find useful:

- If you have typed the address of a legitimate website, check if the address is correct. If the address is incorrect, re-type it and go to the web page again.
- If you have clicked a link in an e-mail or an instant message, verify who sent it to you. If the sender is unknown, this is probably a phishing attempt. If you know the sender, you should check if that person really sent you the link.
- If you reached the web page by browsing the Internet, check the web page where you found the link (click the Back button on your web browser).

If you want to view the web page, click the appropriate link to take one of these actions:

- **View the web page this time only.** There is no risk as long as you do not submit any information on the web page. If the web page is legitimate, you can add it to the White List (click SHIELD DELUXE 2013 Antiphishing toolbar and select **Add to White List**).

- **Add the web page to the White List.** The web page will be displayed immediately and SHIELD DELUXE 2013 will no longer alert you about it.

> *Important*
>
> Add to the White List only the web pages that you fully trust (for example, your bank's web address, known online shops, etc). SHIELD DELUXE 2013 does not check for phishing the web pages in the White List.

You can manage antiphishing protection and the White List using SHIELD DELUXE 2013 toolbar in your web browser. For more information, please refer to "*Managing SHIELD DELUXE 2013 Antiphishing Protection in Internet Explorer and Firefox*" (p. 81).

9.5. Privacy Control Alerts

Privacy Control provides advanced users with some extra features to protect their privacy. You will be prompted for action through specific alert windows if you choose to enable any of these components:

- Registry Control - asks for your permission whenever a program tries to modify a registry entry in order to be executed at Windows start-up.
- Cookie Control - asks for your permission whenever a new website tries to set a cookie.
- Script Control - asks for your permission whenever a website tries to activate a script or other active content.

9.5.1. Registry Alerts

If you enable Registry Control, you will be prompted for permission whenever a new program tries to modify a registry entry in order to be executed at Windows start-up.

You can see the program that is trying to modify Windows Registry.

> *Note*
>
> SHIELD DELUXE 2013 will usually alert you when you install new programs that need to run after the next startup of your computer. In most cases, these programs are legitimate and can be trusted.

If you do not recognize the program and if it seems suspicious, click **Block** to prevent it from modifying Windows Registry. Otherwise, click **Allow** to permit the modification.

Based on your answer, a rule is created and listed in the rules table. The same action is applied whenever this program tries to modify a registry entry.

For more information, please refer to “*Registry Control*” (p. 89).

9.5.2. Script Alerts

If you enable Script Control, you will be prompted for permission whenever a new web site tries to run a script or other active content.

You can see the name of the resource.

Click **Yes** or **No** and a rule will be created, applied and listed in the rules table. The same action will be applied automatically whenever the respective site tries to run active content.

Note
Some web pages may not be properly displayed if you block active content.

For more information, please refer to “*Script Control*” (p. 92).

9.5.3. Cookie Alerts

If you enable Cookie Control, you will be prompted for permission whenever a new web site tries to set or request a cookie.

You can see the name of the application that is trying to send the cookie file.

Click **Yes** or **No** and a rule will be created, applied and listed in the rules table. The same action will be applied automatically whenever you connect to the respective site.

For more information, please refer to “*Cookie Control*” (p. 90).

10. Fixing Issues

SHIELD DELUXE 2013 uses an issue tracking system to detect and inform you about the issues that may affect the security of your computer and data. By default, it will monitor only a series of issues that are considered to be very important. However, you can configure it as needed, choosing which specific issues you want to be notified about.

This is how pending issues are notified:

- A special symbol is displayed over SHIELD DELUXE 2013 2013 icon in the system tray to indicate pending issues.

  Red square with an exclamation mark: Critical issues affect the security of your system. They require your immediate attention and must be fixed as soon as possible.
  Yellow square with an exclamation mark: Non-critical issues affect the security of your system. You should check and fix them when you have the time.
  Also, if you move the mouse cursor over the icon, a pop-up will confirm the existence of pending issues.

- When you open SHIELD DELUXE 2013, the Security Status area will indicate the number of issues affecting your system.
  - In Basic View, the security status is displayed on the left side of the window.
  - In Expert View, go to **General > Dashboard** to check the security status.

10.1. Fix Issues Wizard

The easiest way to fix the existing issues is to follow the **Fix Issues Wizard**. To open the wizard, do any of the following:

- Right-click SHIELD DELUXE 2013 icon in the system tray and select **Fix All Issues**.
- Open SHIELD DELUXE 2013 and, depending on the user interface view mode, proceed as follows:
  - In Basic View, click **View All Issues**.
  - In Expert View, go to **General > Dashboard** and click **View All Issues**.

> *Note*
> You can also add a shortcut to My Tools.

A list of existing security threats on your computer is displayed.

All current issues are selected to be fixed. If there is an issue that you do not want to be fixed, just clear the corresponding check box. If you do so, its status will change to **Skip**.

> *Note*
> If you do not want to be notified about specific issues, you must configure the alert system accordingly, as described in the next section.

To fix the selected issues, click **Start**. Some issues are fixed immediately. For others, a wizard helps you fix them.

The issues that this wizard helps you fix can be grouped into these main categories:

- **Disabled security settings.** Such issues are fixed immediately, by enabling the respective security settings.
- **Preventive security tasks you need to perform.** An example of such a task is scanning your computer. It is recommended that you scan your computer at least once a week. SHIELD DELUXE 2013 will automatically do that for you in most cases. However, if you have changed the scanning schedule or if the schedule is not completed, you will be notified about this issue.

  When fixing such issues, a wizard helps you successfully complete the task.
- **System vulnerabilities.** SHIELD DELUXE 2013 automatically checks your system for vulnerabilities and alerts you about them. System vulnerabilities include the following:
  - weak passwords to Windows user accounts.
  - outdated software on your computer.
  - missing Windows updates.
  - Windows Automatic Updates is disabled.

  When such issues are to be fixed, the vulnerability scan wizard is started. This wizard assists you in fixing the detected system vulnerabilities. For detailed information, please refer to section "*Checking for Vulnerabilities*" (p. 94).

10.2. Configuring Status Alerts

The status alert system is pre-configured to monitor and alert you about the most important issues that may affect the security of your computer and data. Besides the issues monitored by default, there are several other issues you can be informed about.

You can configure the alert system to best serve your security needs by choosing which specific issues to be informed about. You can do this either in Intermediate View or in Expert View.

- In Intermediate View, the alert system can be configured from separate locations. Follow these steps:
  1. Go to the **Security** tab.
  2. Click the **Add/Edit List** link in the Status area.
  3. Use the switch corresponding to an item to change its alert state.
- In Expert View, the alert system can be configured from a central location. Follow these steps:
  1. Go to **General > Dashboard**.
  2. Click **Add/Edit Alerts**.
  3. Use the switch corresponding to an item to change its alert state.

11. Configuring Main Settings

You can configure the main product settings (including reconfiguring the usage profile) from the Preferences window. To open it, do any of the following:

- Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Preferences**.
- Right-click SHIELD DELUXE 2013 icon ● in the system tray and select **Preferences**.

Note

To configure the product settings in detail, use the Expert View interface. For detailed information, please refer to the "Configuration and Management" (p. 48) part of this user guide.

The settings are organized into three categories:

- Security Settings
- Alerts Settings
- General Settings

To turn on or off a setting, use the corresponding switch.

To apply and save the configuration changes you make, click **OK**. To close the window without saving the changes, click **Cancel**.

The **Reconfigure Profile** link in the upper-right corner of the window allows you to reconfigure the usage profile. For more information, please refer to "*Reconfiguring the Usage Profile*" (p. 43).

11.1. Security Settings

In this area, you can enable or disable product settings that cover various aspects of computer and data security. To turn on or off a setting, use the corresponding switch.

Warning

Use caution when disabling real-time antivirus protection or automatic update. Disabling these features may compromise your computer's security. If you really need to disable them, remember to re-enable them as soon as possible.

These are the available settings:

Antivirus

Real-time protection ensures that all files are scanned as they are accessed by you or by an application running on this system.

Automatic Update

Automatic update ensures that the newest SHIELD DELUXE 2013 product and signature files are downloaded and installed automatically, on a regular basis. Updates are performed by default every hour.

Vulnerability Scan

Automatic Vulnerability Scan alerts you about and helps you fix vulnerabilities in your system that might affect its security. Such vulnerabilities include outdated software, weak passwords to user accounts or missing Windows updates.

Antiphishing

Antiphishing detects and alerts you in real-time if a web page is set up to steal personal information.

Search Advisor

Search Advisor scans the links in your search results and informs you which of them are safe and which are not.

Identity Control

Identity Control helps you prevent your personal data from being sent out on the Internet without your consent. It blocks any instant messages, e-mail messages or web forms transmitting data you defined as being private to unauthorized recipients (addresses).

Chat Encryption

Chat Encryption secures your conversations via Yahoo! Messenger and Windows Live Messenger provided that your IM contacts use a compatible SHIELD DELUXE 2013 product and IM software.

The status of some of these settings may be monitored by SHIELD DELUXE 2013 issue tracking system. If you disable a monitored setting, SHIELD DELUXE 2013 will indicate this as an issue that you need to fix.

If you do not want a monitored setting that you disabled to be shown as an issue, you must configure the tracking system accordingly. You can do that either in Intermediate View or in Expert View. For detailed information, please refer to "*Configuring Status Alerts*" (p. 38).

11.2. Alerts Settings

In this area, you can turn off SHIELD DELUXE 2013 pop-ups and alerts. SHIELD DELUXE 2013 uses alerts to prompt you for action and pop-ups to inform you about actions it has taken automatically or about other events. To turn on or off a category of alerts, use the corresponding switch.

Important

Most of these alerts and pop-ups should be kept turned on in order to avoid potential problems.

These are the available settings:

Antivirus Alerts

Antivirus alerts inform you when SHIELD DELUXE 2013 detects and blocks a virus. When a virus is detected, it is best practice to scan the entire computer to make sure there are no other viruses.

Active Virus Control Pop-ups

If you are using the Basic View or Intermediate View interface, a pop-up will inform you whenever Active Virus Control blocks a potentially harmful application. If you are using Expert View, you will be prompted for action, through an alert window, when an application exhibits malicious behavior.

Scan Email Pop-ups

These pop-ups are displayed to inform you that SHIELD DELUXE 2013 is scanning e-mails for malware.

Home Network Management Alerts

These alerts inform the user when administrative actions are being performed remotely.

Quarantine Alerts

Quarantine alerts inform you when old quarantined files have been deleted.

Registration Pop-ups

Registration pop-ups are used to remind you that you need to register The Shield Deluxe or to inform you that the license key is about to or has already expired.

11.3. General Settings

In this area, you can enable or disable settings that affect product behavior and user experience. To turn on or off a setting, use the corresponding switch.

These are the available settings:

Game Mode

Game Mode temporarily modifies protection settings so as to minimize their impact on system performance during games.

Laptop Mode Detection

Laptop Mode temporarily modifies protection settings so as to minimize their impact on the life of your laptop battery.

Settings Password

To prevent someone else from changing SHIELD DELUXE 2013 settings, you can protect them with a password. When you enable this option, you will be prompted to configure the settings password. Type the desired password in both fields and click **OK** to set the password.

SHIELD DELUXE 2013 News

By enabling this option, you will receive important company news, product updates or new security threats from SHIELD DELUXE 2013.

Product Notification Alerts

By enabling this option, you will receive information alerts.

Scan Activity Bar

The Scan Activity Bar is a small, transparent window indicating the progress of SHIELD DELUXE 2013 scanning activity.

Send Virus Reports

By enabling this option, virus scanning reports are sent to SHIELD DELUXE 2013 labs for analysis. Please note that these reports will contain no confidential data, such as your name or IP address, and that they will not be used for commercial purposes.

Outbreak Detection

By enabling this option, reports regarding potential virus-outbreaks are sent to SHIELD DELUXE 2013 labs for analysis. Please note that these reports will contain no confidential data, such as your name or IP address, and that they will not be used for commercial purposes.

11.4. Reconfiguring the Usage Profile

During installation, you were able to configure a usage profile. The usage profile reflects the main activities performed on the computer. Depending on the usage profile, the product interface is organized to allow easy access to your preferred tasks.

To reconfigure the usage profile, click **Reconfigure Profile** and follow the configuration wizard. You can navigate through the wizard using the **Next** and **Back** buttons. To exit the wizard, click **Cancel**.

1. **Choose Your View**

   Select the preferred user interface view.

2. **Configure My Tools**

   If you have selected Basic View or Intermediate View, choose the features you would like to create shortcuts to on the Dashboard.

3. **Configure Settings**

   If you have selected Expert View, configure SHIELD DELUXE 2013 settings as needed. To turn on or off a setting, use the corresponding switch.

4. **Home Network Management**

   Note
   This step appears only if you have added Home Network Management to My Tools.

   You can select one of three options:

   - **Set up this PC as "Server"**

     Select this option if you intend to manage SHIELD DELUXE 2013 products on other computers in the home network from this one.

     A password is required to join the network. Enter the password in the provided text boxes and click **Submit**.

   - **Set up this PC as "Client"**

     Select this option if SHIELD DELUXE 2013 will be managed from another computer in the home network which is also running SHIELD DELUXE 2013.

     A password is required to join the network. Enter the password in the provided text boxes and click**Submit**.

   - **Skip setup for now**

     Select this option to configure this feature at a later time from the The Shield Deluxe window.

5. **Setup Complete**

   Click **Finish**.

12. History and Events

The **View Logs** link at the bottom of SHIELD DELUXE 2013 main window opens another window with SHIELD DELUXE 2013 history & events. This window offers you an overview of the security-related events. For instance, you can easily check if the update was successfully performed, if malware was found on your computer etc.

In order to help you filter SHIELD DELUXE 2013 history & events, the following categories are provided on the left side:

- **Dashboard**
- **Antivirus**
- **Privacy Control**
- **Vulnerability**
- **Chat encryption**
- **Game/Laptop Mode**
- **Home Network**
- **Update**
- **Registration**

A list of events is available for each category. Each event comes with the following information: a short description, the action SHIELD DELUXE 2013 took on it when it happened, and the date and time when it occurred. If you want to find out more information about a particular event in the list, double-click that event.

Click **Clear all logs** if you want to remove old logs or **Refresh** to make sure the latest logs are displayed.

13. Registration

SHIELD DELUXE 2013 comes with 14-day trial period. During the trial period, the product is fully functional and you can test it to see if it meets your expectations.

Before the trial period is over, you must register the product with a license key in order to keep your computer protected. The license key specifies how long you are entitled to use the product. As soon as the license key expires, SHIELD DELUXE 2013 stops performing its functions and protecting your computer. You should purchase a license key or renew your license a few days before the current license key expires.

13.1. Registering SHIELD DELUXE 2013

If you want to register the product with a license key or to change the current license key, click the **License Info** link, located at the bottom of SHIELD DELUXE 2013 window. The product registration window will appear.

You can see SHIELD DELUXE 2013 registration status, the current license key and how many days are left until the license expires.

To register SHIELD DELUXE 2013:

1. Type the license key in the edit field.

   Note
   You can find your license key:
   - on the "Thank You" page after your order.
   - in your order confirmation e-mail.
   - at the PCSecurityShield customer center.

   If you do not have a license key for SHIELD DELUXE 2013, click the provided link to go to the online store and buy one.

2. Click **Register Now**.
3. Click **Finish**.

13.2. Buying or Renewing License Keys

If the trial period is going to end soon, you must purchase a license key and register your product. Similarly, if your current license key is going to expire soon, you must renew your license.

To purchase a new license key or renew an existing license, open SHIELD DELUXE 2013 in Intermediate View or Expert View and click the **Buy** / **Renew** link located at the bottom of the window.

Configuration and Management

14. General Settings

The General module provides information on SHIELD DELUXE 2013 activity and the system. Here you can also change the overall behavior of SHIELD DELUXE 2013.

To configure the general settings:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **General > Settings**.

- **Enable password protection for product settings** - enables setting a password in order to protect SHIELD DELUXE 2013 configuration.

  Note
  If you are not the only person with administrative rights using this computer, it is recommended that you protect your SHIELD DELUXE 2013 settings with a password.

  Type the password in the **Password** field, re-type it in the **Retype password** field and click **OK**.

  Once you have set the password, you will be asked for it whenever you want to change SHIELD DELUXE 2013 settings. The other system administrators (if any) will also have to provide this password in order to change SHIELD DELUXE 2013 settings.

  Important
  If you forgot the password you will have to repair the product in order to modify the SHIELD DELUXE 2013 configuration.

- **Show SHIELD DELUXE 2013 News (security related notifications)** - shows from time to time security notifications regarding virus outbreaks, sent by SHIELD DELUXE 2013 server.
- **Show pop-ups (on-screen notes)** - shows pop-up windows regarding the product status. You can configure SHIELD DELUXE 2013 to display pop-ups only when the interface is in Basic / Intermediate View or in Expert View.
- **Show the Scan Activity bar (on screen graph of product activity)** - displays the Scan Activity bar whenever you log on to Windows. Clear this check box if you do not want the Scan Activity bar to be displayed anymore.

Note

The Scan activity bar is only available when the interface is in Expert View.

Virus Report Settings

- **Send virus reports** - sends to SHIELD DELUXE 2013 Labs reports regarding viruses identified in your computer. It helps us keep track of virus-outbreaks.

  The reports will contain no confidential data, such as your name, IP address or others, and will not be used for commercial purposes. The information supplied will contain only the virus name and will be used solely to create statistic reports.

- **Enable SHIELD DELUXE 2013 Outbreak Detection** - sends to SHIELD DELUXE 2013
  Labs reports regarding potential virus-outbreaks.

  The reports will contain no confidential data, such as your name, IP address or others, and will not be used for commercial purposes. The information supplied will contain only the potential virus and will be used solely to detect new viruses.

Connection Settings

Several SHIELD DELUXE 2013 components (the Firewall, LiveUpdate, Real-Time Virus Reporting and Real-Time Spam Reporting modules) require access to the Internet. SHIELD DELUXE 2013 comes with a proxy manager that allows configuring from one location the proxy settings used by SHIELD DELUXE 2013 components to access the Internet.

If your company uses a proxy server to connect to the Internet, you must specify the proxy settings in order for SHIELD DELUXE 2013 to update itself. Otherwise, it will use the proxy settings of the administrator that installed the product or of the current user's default browser, if any. For more information, please refer to “*How Do I Find Out My Proxy Settings?*” (p. 140).

Note

The proxy settings can be configured only by users with administrative rights on the computer or by power users (users who know the password to the product settings).

To manage the proxy settings, click **Proxy Settings**.

There are three sets of proxy settings:

- **Proxy Detected at Install Time** - proxy settings detected on the administrator's account during installation and which can be configured only if you are logged on to that account. If the proxy server requires a username and a password, you must specify them in the corresponding fields.
- **Default Browser Proxy** - proxy settings of the current user, extracted from the default browser. If the proxy server requires a username and a password, you must specify them in the corresponding fields.

> *Note*
> The supported web browsers are Internet Explorer, Mozilla Firefox and Opera. If you use another browser by default, SHIELD DELUXE 2013 will not be able to obtain the proxy settings of the current user.

- **Custom Proxy** - proxy settings that you can configure if you are logged in as an administrator.

  The following settings must be specified:
  - **Address** - type in the IP of the proxy server.
  - **Port** - type in the port SHIELD DELUXE 2013 uses to connect to the proxy server.
  - **Username** - type in a user name recognized by the proxy.
  - **Password** - type in the valid password of the previously specified user.

SHIELD DELUXE 2013 will use the proxy settings sets in the following order until it manages to connect to the Internet:

1. the specified proxy settings.
2. the proxy settings detected at install time.
3. the proxy settings of the current user.

When trying to connect to the Internet, each set of proxy settings is tried at a time, until SHIELD DELUXE 2013 manages to connect.

First, the set containing your own proxy settings will be used to connect to the Internet. If it does not work, the proxy settings detected at installation time will be tried next. Finally, if those do not work either, the proxy settings of the current user will be taken from the default browser and used to connect to the Internet.

Click **OK** to save the changes and close the window.

Click **Apply** to save the changes or click **Default** to load the default settings.

System Information

SHIELD DELUXE 2013 allows you to view, from a single location, all system settings and the applications registered to run at startup. In this way, you can monitor the activity of the system and of the applications installed on it as well as identify possible system infections.

To obtain system information:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **General > System Info**.

The list contains all the items loaded when starting the system as well as the items loaded by different applications.

Three buttons are available:

- **Restore** - changes a current file association to default. Available for the **File Associations** settings only!
- **Go to** - opens a window where the selected item is placed (the **Registry** for example).

Note
Depending on the selected item, the **Go to** button may not appear.

- **Refresh** - re-opens the **System Info** section.

Optimization

The Optimization tab is useful when you wish to run an on-demand scan without being disturbed from your work.

For example, if you want to run a Deep System Scan this may take some time if you have many items on your hard disk or if your system configuration doesn't meet the recommended requirements.

To access the Optimization tab:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.

2. Go to **General > Optimization**.

System load is constantly being monitored. When the system enters an idle state The Shield Deluxe can launch:

- **Deep System Scan**
- **Quick Scan**
- **Full System Scan**
- **My Documents Scan**

Note
Select **Update product before running this task** check box to make sure you have the latest virus definitions.

15. Antivirus Protection

SHIELD DELUXE 2013 protects your computer from all kinds of malware (viruses, Trojans, spyware, rootkits and so on). The protection SHIELD DELUXE 2013 offers is divided into two categories:

- Real-time protection - prevents new malware threats from entering your system. SHIELD DELUXE 2013 will, for example, scan a word document for known threats when you open it, and an e-mail message when you receive one.

  Real-time protection is also referred to as on-access scanning - files are scanned as the users access them.

  Important
  To prevent viruses from infecting your computer keep **Real-time protection** enabled.

- On-demand scanning - allows detecting and removing the malware that already resides in the system. This is the classic scan initiated by the user - you choose what drive, folder or file SHIELD DELUXE 2013 should scan, and SHIELD DELUXE 2013 scans it - on-demand. The scan tasks allow you to create customized scanning routines and they can be scheduled to run on a regular basis.

When it detects a virus or other malware, SHIELD DELUXE 2013 will automatically attempt to remove the malware code from the infected file and reconstruct the original file. This operation is referred to as disinfection. Files that cannot be disinfected are moved to quarantine in order to contain the infection. For more information, please refer to "*Quarantine Area*" (p. 78).

If your computer has been infected with malware, please refer to "*Removing Malware from Your System*" (p. 130).

Advanced users can configure scan exclusions if they do not want specific files to be scanned. For more information, please refer to "*Configuring Scan Exclusions*" (p. 74).

15.1. Real-time Protection

SHIELD DELUXE 2013 provides continuous, real-time protection against a wide range of malware threats by scanning all accessed files, e-mail messages and the communications through Instant Messaging Software applications (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

The default real-time protection settings ensure good protection against malware, with minor impact on system performance. You can easily change the real-time protection settings according to your needs by switching to one of the predefined protection levels. Or, if you are an advanced user, you can configure the scan settings in detail by creating a custom protection level.

To learn more, please refer to these topics:

- "*Adjusting the Real-time Protection Level*" (p. 55)
- "*Creating a Custom Protection Level*" (p. 56)
- "*Changing the Actions Taken on Detected Files*" (p. 57)
- "*Restoring the Default Settings*" (p. 59)

To protect you against unknown malicious applications, SHIELD DELUXE 2013 uses an advanced heuristic technology (Active Virus Control) and an Intrusion Detection System, which continuously monitor your system. To learn more, please refer to these topics:

- "*Configuring Active Virus Control*" (p. 59)
- "*Configuring the Intrusion Detection System*" (p. 61)

15.1.1. Adjusting the Real-time Protection Level

The real-time protection level defines the scan settings for real-time protection. You can easily change the real-time protection settings according to your needs by switching to one of the predefined protection levels.

To adjust the real-time protection level:

1. Open SHIELD DELUXE
2013.

2. Depending on the user interface view mode, proceed as follows:

Intermediate View
    Go to the **Security** tab and click **Configure Antivirus** in the Quick Tasks area on the left side of the window.

    Go to the **Shield** tab.

Expert View
    Go to **Antivirus > Shield**.

Note

In Basic View and Intermediate View, you can configure a shortcut so that you can access these settings from your dashboard. For more information, please refer to "*My Tools*" (p. 29).

3. Drag the slider along the scale to set the desired protection level. Use the description on the right side of the scale to choose the protection level that better fits your security needs.

15.1.2. Creating a Custom Protection Level

Advanced users might want to take advantage of the scan settings SHIELD DELUXE 2013 offers. The scanner can be set to scan only specific file extensions, to search for specific malware threats or to skip archives. This may greatly reduce scanning times and improve your computer's responsiveness during a scan.

You can configure the real-time protection settings in detail by creating a custom protection level. To create a custom protection level:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus > Shield**.
3. Click **Custom Level**.
4. Configure the scan settings as needed. To find out what an option does, keep the mouse over it and read the description displayed at the bottom of the window.
5. Click **OK** to save the changes and close the window.

You may find this information useful:

- If you are not familiar with some of the terms, check them in the glossary. You can also find useful information by searching the Internet.
- **Scan accessed files.** You can set SHIELD DELUXE 2013 to scan all accessed files, applications (program files) only or specific file types you consider to be dangerous. Scanning all accessed files provides best protection, while scanning applications only can be used for better system performance.

  Applications (or program files) are far more vulnerable to malware attacks than other types of files. This category includes the following file extensions: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`;

`.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml`; `.nws`.

If you opt for **Scan user defined extensions**, it is recommended that you include all application extensions beside other file extensions you consider to be dangerous.

- **Scan only new and changed files.** By scanning only new and changed files, you may greatly improve overall system responsiveness with a minimum trade-off in security.
- **Scan inside archives.** Scanning inside archives is a slow and resource-intensive process, which is therefore not recommended for real-time protection. Archives containing infected files are not an immediate threat to the security of your system. The malware can affect your system only if the infected file is extracted from the archive and executed without having real-time protection enabled.
- **Action options.** If you consider changing the actions taken on detected files, check for tips in "*Changing the Actions Taken on Detected Files*" (p. 57).
- **Scan options for e-mail, web and instant messaging traffic.** To prevent malware from being downloaded to your computer, SHIELD DELUXE 2013 automatically scans the following malware entry points:
  - incoming e-mails
  - web traffic
  - files received via Yahoo! Messenger and Windows Live Messenger

  Scanning the web traffic may slow down web browsing a little, but it will block malware coming from the Internet, including drive-by downloads.

  Though not recommended, you can disable e-mail, web or instant messaging antivirus scan to increase system performance. If you disable the corresponding scan options, the e-mails and files received or downloaded from the Internet will not be scanned, thus allowing infected files to be saved to your computer. This is not a major threat because real-time protection will block the malware when the infected files are accessed (opened, moved, copied or executed).

15.1.3. Changing the Actions Taken on Detected Files

Files detected by real-time protection are grouped into two categories:

- **Infected files.** Files detected as infected match a malware signature in the The Shield Deluxe Malware Signature Database. SHIELD DELUXE 2013 can normally remove the malware code from an infected file and reconstruct the original file. This operation is known as disinfection.

> *Note*
> Malware signatures are snippets of code extracted from actual malware samples. They are used by antivirus programs to perform pattern-matching and detect malware. SHIELD DELUXE 2013 Malware Signature Database is a collection of malware signatures updated hourly by SHIELD DELUXE 2013 malware researchers.

- **Suspicious files.** Files are detected as suspicious by the heuristic analysis. Suspicious files cannot be disinfected, because no disinfection routine is available.

Depending on the type of detected file, the following actions are taken automatically:

- If an infected file is detected, SHIELD DELUXE 2013 will automatically attempt to disinfect it. If disinfection fails, the file is moved to quarantine in order to contain the infection.

  > *Important*
  > For particular types of malware, disinfection is not possible because the detected file is entirely malicious. In such cases, the infected file is deleted from the disk.

- If a suspicious file is detected, access to that file will be denied to prevent a potential infection.

You should not change the default actions taken on detected files unless you have a strong reason to do so.

To change the default actions taken on the infected or suspicious files detected:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus > Shield**.
3. Click **Custom Level**.
4. Configure the actions to be taken on each category of detected files, as needed. The second action is taken if the first one fails (for example, if disinfection is not possible, the infected file is moved to quarantine).

15.1.4. Restoring the Default Settings

The default real-time protection settings ensure good protection against malware, with minor impact on system performance.

To restore the default real-time protection settings:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus > Shield**.
3. Click **Default Level**.

15.1.5. Configuring Active Virus Control

SHIELD DELUXE 2013 Active Virus Control detects potentially harmful applications based on their behavior.

Active Virus Control continuously monitors the applications running on the computer, looking for malware-like actions. Each of these actions is scored and an overall score is computed for each process. When the overall score for a process reaches a given threshold, the process is considered to be harmful. Depending on the program settings, the process is blocked automatically or you may prompted to specify the action to be taken.

Active Virus Control can be configured to alert you and prompt you for action whenever an application tries to perform a possible malicious action.

If you know and trust the detected application, click **Allow**.

If you want to immediately close the application, click **OK**.

Select the **Remember this action for this application** check box before making your choice and SHIELD DELUXE 2013 will take the same action for the detected application in the future. The rule that is thus created will be listed in the Active Virus Control configuration window.

To configure Active Virus Control:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus > Shield**.
3. Click **Advanced Settings**.

4. Go to the **AVC** tab.
5. Select the corresponding check box to enable Active Virus Control.
6. Drag the slider along the scale to set the desired protection level. Use the description on the right side of the scale to choose the protection level that better fits your security needs.

Adjusting the Aggressiveness Level

To configure the Active Virus Control protection level:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus > Shield**.
3. Click **Advanced Settings**.
4. Go to the **AVC** tab.
5. Drag the slider along the scale to set the desired protection level. Use the description on the right side of the scale to choose the protection level that better fits your security needs.

Configuring the Response to Malicious Behavior

If an application exhibits malicious behavior, you will be prompted whether to allow or block it.

To configure the response to malicious behavior:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus > Shield**.
3. Click **Advanced Settings**.
4. Go to the **AVC** tab.
5. If you want to be prompted for action when Active Virus Control detects a potentially harmful application, select the **Alert me before taking an action** check box. To automatically block an application that exhibits malicious behavior (without displaying an alert window), clear this check box.

Managing Trusted / Untrusted Applications

You can add applications you know and trust to the list of trusted applications. These applications will no longer be checked by SHIELD DELUXE 2013 Active Virus Control and will automatically be allowed access.

To manage the applications that are not being monitored by Active Virus Control:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus > Shield**.
3. Click **Advanced Settings**.
4. Go to the **AVC** tab.
5. Click the **Exclusions** tab.

The applications for which rules have been created are listed in the **Exclusions** table. The path to the application and the action you have set for it (Allowed or Blocked) is displayed for each rule.

To change the action for an application, click the current action and select the other action from the menu.

To manage the list, use the buttons placed above the table:

- **Add** - add a new application to the list.
- **Remove** - remove an application from the list.
- **Edit** - edit an application rule.

15.1.6. Configuring the Intrusion Detection System

SHIELD DELUXE 2013 Intrusion Detection System monitors network and system activities for malicious activities or policy violations.

To configure the Intrusion Detection System:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus > Shield**.
3. Click **Advanced Settings**.
4. Go to the **IDS** tab.

5. Select the corresponding check box to enable the Intrusion Detection System.
6. Drag the slider along the scale to set the desired aggressiveness level. Use the description on the right side of the scale to choose the aggressiveness level that better fits your security needs.

15.2. On-demand Scanning

The main objective for SHIELD DELUXE 2013 is to keep your computer clean of viruses. This is first and foremost done by keeping new viruses out of your computer and by scanning your e-mail messages and any new files downloaded or copied to your system.

There is a risk that a virus is already lodged in your system, before you even install SHIELD DELUXE 2013. This is why it's a very good idea to scan your computer for resident viruses after you've installed SHIELD DELUXE 2013. And it's definitely a good idea to frequently scan your computer for viruses.

On-demand scanning is based on scan tasks. Scan tasks specify the scanning options and the objects to be scanned. You can scan the computer whenever you want by running the default tasks or your own scan tasks (user-defined tasks). You can also schedule them to run on a regular basis or when the system is idle so as not to interfere with your work. For quick instructions, please refer to these topics:

- "*How Do I Scan Files and Folders?*" (p. 114)
- "*How Do I Create a Custom Scan Task?*" (p. 117)
- "*How Do I Schedule a Computer Scan?*" (p. 119)

15.2.1. Scanning Files and Folders

You should scan files and folders whenever you suspect they might be infected. Right-click the file or folder you want to be scanned and select **Scan with SHIELD DELUXE 2013**. The Antivirus Scan wizard will appear and guide you through the scanning process.

If you want to scan specific locations on your computer, you can configure and run a custom scan task. For more information, please refer to "*How Do I Create a Custom Scan Task?*" (p. 117).

To scan your computer or part of it you can run the default scan tasks or your own scan tasks. To run a scan task, open SHIELD DELUXE 2013 and, depending on the user interface view mode, proceed as follows:

Basic View

Click the **Security** button and choose one of the available scan tasks.

Intermediate View

Go to the **Security** tab. Click **Full System Scan** in the left-side Quick Tasks area and choose one of the available scan tasks.

Expert View

Go to **Antivirus > Virus Scan**. To run a system or user-defined scan task, click the corresponding **Run Task** button.

These are the default tasks you can use to scan your computer:

Full System Scan

Scans the entire system, except for archives. In the default configuration, it scans for all types of malware other than rootkits.

Quick Scan

Quick Scan uses in-the-cloud scanning to detect malware running in your system. Running a Quick Scan usually takes less than a minute and uses a fraction of the system resources needed by a regular virus scan.

Deep System Scan

Scans the entire system. In the default configuration, it scans for all types of malware threatening your system's security, such as viruses, spyware, adware, rootkits and others.

Before you initiate a scanning process, you should make sure that SHIELD DELUXE 2013 is up to date with its malware signatures. Scanning your computer using an outdated signature database may prevent SHIELD DELUXE 2013 from detecting new malware found since the last update.

In order for SHIELD DELUXE 2013 to make a complete scanning, you need to shut down all open programs. Especially your email-client (i.e. Outlook, Outlook Express or Eudora) is important to shut down.

Scanning Tips

Here are some more scanning tips you may find useful:

- Depending on the size of your hard disk, running a comprehensive scan of your computer (such as Deep System Scan or System Scan) may take a while (up to an hour or even more). Therefore, you should run such scans when you do not need to use your computer for a longer time (for example, during the night).

You can schedule the scan to start when convenient. Make sure you leave your computer running. With Windows Vista, make sure your computer is not in sleep mode when the task is scheduled to run.

- If you frequently download files from the Internet to a specific folder, create a new scan task and set that folder as scan target. Schedule the task to run every day or more often.
- There is a kind of malware which sets itself to be executed at system startup by changing Windows settings. To protect your computer against such malware, you can schedule the **Auto-logon Scan** task to run at system startup. Please note that autologon scanning may affect system performance for a short time after startup.

15.2.2. Antivirus Scan Wizard

Whenever you initiate an on-demand scan (for example, right-click a folder and select **Scan with SHIELD DELUXE 2013**), SHIELD DELUXE 2013 Antivirus Scan wizard will appear. Follow the three-step guided procedure to complete the scanning process.

Note

If the scan wizard does not appear, the scan may be configured to run silently, in the background. Look for the ● scan progress icon in the system tray. You can click this icon to open the scan window and to see the scan progress.

Step 1/3 - Scanning

SHIELD DELUXE 2013 will start scanning the selected objects.

You can see the scan status and statistics (scanning speed, elapsed time, number of scanned / infected / suspicious / hidden objects and other).

Wait for SHIELD DELUXE 2013 to finish scanning.

Note

The scanning process may take a while, depending on the complexity of the scan.

Password-protected archives. When a password-protected archive is detected, depending on the scan settings, you may be prompted to provide the password. Password-protected archives cannot be scanned unless you provide the password. The following options are available:

- **I want to enter the password for this object.** If you want SHIELD DELUXE 2013 to scan the archive, select this option and type the password. If you do not know the password, choose one of the other options.
- **I do not want to enter the password for this object (skip this object).** Select this option to skip scanning this archive.
- **I do not want to enter the password for any object (skip all password-protected objects).** Select this option if you do not want to be bothered about password-protected archives. SHIELD DELUXE 2013 will not be able to scan them, but a record will be kept in the scan log.

Click **OK** to continue scanning.

Stopping or pausing the scan. You can stop scanning anytime you want by clicking **Stop&Yes**. You will go directly to the last step of the wizard. To temporarily stop the scanning process, just click **Pause**. You will have to click **Resume** to resume scanning.

Step 2/3 - Select Actions

When the scanning is completed, a new window will appear, where you can see the scan results.

If there are no unresolved threats, click **Continue**. Otherwise, you must configure new actions to be taken on the unresolved threats in order to protect your system.

The infected objects are displayed in groups, based on the malware they are infected with. Click the link corresponding to a threat to find out more information about the infected objects.

You can choose an overall action to be taken for all issues or you can select separate actions for each group of issues. One or several of the following options can appear on the menu:

Take No Action

No action will be taken on the detected files. After the scan is completed, you can open the scan log to view information on these files.

Disinfect

Removes the malware code from infected files.

Delete

Removes detected files from the disk.

Move to quarantine

Moves detected files to quarantine. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. For more information, please refer to "*Quarantine Area*" (p. 78).

Rename files

Changes the name of hidden files by appending `.bd.ren` to their name. As a result, you will be able to search for and find such files on your computer, if any.

Please note that these hidden files are not the files that you deliberately hide from Windows. They are the files hidden by special programs, known as rootkits. Rootkits are not malicious in nature. However, they are commonly used to make viruses or spyware undetectable by normal antivirus programs.

Click **Continue** to apply the specified actions.

Step 3/3 - View Results

When SHIELD DELUXE 2013 finishes fixing the issues, the scan results will appear in a new window. If you want comprehensive information on the scanning process, click **Show Log** to view the scan log.

Important

If required, please restart your system in order to complete the cleaning process.

Click **Close** to close the window.

SHIELD DELUXE 2013 Could Not Solve Some Issues

In most cases SHIELD DELUXE 2013 successfully disinfects the infected files it detects or it isolates the infection. However, there are issues that cannot be solved automatically. For more information and instructions on how to remove malware manually, please refer to "*Removing Malware from Your System*" (p. 130).

SHIELD DELUXE 2013 Detected Suspect Files

Suspect files are files detected by the heuristic analysis as potentially infected with malware the signature of which has not been released yet.

If suspect files were detected during the scan, you will be requested to submit them to SHIELD DELUXE 2013 Lab. Click **OK** to send these files to SHIELD DELUXE 2013 Lab for further analysis.

15.2.3. Viewing Scan Logs

Each time you perform a scan, a scan log is created. The scan log contains detailed information about the logged scanning process, such as scanning options, the scanning target, the threats found and the actions taken on these threats.

You can open the scan log directly from the scan wizard, once the scan is completed, by clicking **Show Log**.

To check scan logs at a later time:

1. Open SHIELD DELUXE 2013.
2. Click the **View Logs** link in the bottom-right corner of the window.
3. Click **Antivirus** on the left-side menu.
4. In the **On-demand Tasks** section, you can check what scans have been performed recently. Double-click the events in the list to see more details. To open the scan log, click **View Scan Log**. The scan log will open in your default web browser.

To delete a log entry, right-click it and select **Delete**.

15.2.4. Managing Existing Scan Tasks

SHIELD DELUXE 2013 comes with several tasks, created by default, which cover common security issues. You can also create your own customized scan tasks. For more information, please refer to "*How Do I Create a Custom Scan Task?*" (p. 117).

To manage the existing scan tasks:

1. Open SHIELD DELUXE 2013.
2. Depending on the user interface view mode, proceed as follows:

   Intermediate View

   Go to the **Security** tab and click **Configure Antivirus** in the Quick Tasks area on the left side of the window.

   Go to the **Virus Scan** tab.

   Expert View

   Go to **Antivirus > Virus Scan**.

Note

In Basic View and Intermediate View, you can configure a shortcut so that you can access these settings from your dashboard. For more information, please refer to "*My Tools*" (p. 29).

There are three categories of scan tasks:

- **System tasks** - contains the list of default system tasks. The following tasks are available:

  Full System Scan

  Scans the entire system, except for archives. In the default configuration, it scans for all types of malware other than rootkits.

  Quick Scan

  Quick Scan uses in-the-cloud scanning to detect malware running in your system. Running a Quick Scan usually takes less than a minute and uses a fraction of the system resources needed by a regular virus scan.

  Auto-logon Scan

  Scans the items that are run when a user logs on to Windows. By default, the autologon scan is disabled.

  If you want to use this task, right-click it, select **Schedule** and set the task to run **at system startup**. You can specify how long after the startup the task should start running (in minutes).

  Deep System Scan

  Scans the entire system. In the default configuration, it scans for all types of malware threatening your system's security, such as viruses, spyware, adware, rootkits and others.

  Note

  Since the **Deep System Scan** and **Full System Scan** tasks analyze the entire system, the scanning may take a while. Therefore, we recommend you to run these tasks on low priority or, better, when your system is idle.

- **User tasks** - contains the user-defined tasks.

  A task called `My Documents` is provided. Use this task to scan important current user folders: `My Documents`, `Desktop` and `StartUp`. This will ensure the safety of your documents, a safe workspace and clean applications running at startup.

- **Misc tasks** - contains a list of miscellaneous scan tasks. These scan tasks refer to alternative scanning types that cannot be run from this window. You can only modify their settings or view the scan reports. The following tasks are available:

  Device Scanning

  SHIELD DELUXE 2013 can detect automatically when a new storage device is connected to the computer and scan it. Use this task to configure the options of the automatic detection and scanning of storage devices (CDs/DVDs, USB storage devices or mapped network drives).

  Contextual Scan

  This task is used when scanning via the Windows contextual menu or using the scan activity bar. You can modify the scan options to better suit your needs.

You can manage scan tasks using the buttons or the shortcut menu.

To run a system or user-defined scan task, click the corresponding **Run Task** button. The Antivirus Scan wizard will appear and guide you through the scanning process.

To set a scan task to run automatically, at a later moment or regularly, click the corresponding **Schedule** button and configure the task schedule as needed.

If you no longer need a scan task that you have created (a user-defined task), you can delete it by clicking the ⊗ **Delete** button, located to the right of the task. You cannot remove system or miscellaneous tasks.

Each scan task has a Properties window where you can configure its settings and view the scan logs. To open this window click the **Properties** button to the left of the task (or right-click the task and then click **Properties**).

To learn more, please refer to these topics:

- "*Configuring Scan Settings*" (p. 70)
- "*Setting Scan Target*" (p. 73)
- "*Scheduling Scan Tasks*" (p. 73)

Using Shortcut Menu

A shortcut menu is available for each task. Right-click the selected task to open it.

For system and user-defined tasks, the following commands are available on the shortcut menu:

- **Scan Now** - runs the selected task, initiating an immediate scan.

- **Paths** - opens the **Properties** window, Paths tab, where you can change the scan target of the selected task. In the case of system tasks, this option is replaced by **Show Scan Paths**, as you can only see their scan target.
- **Schedule** - opens the **Properties** window, Scheduler tab, where you can schedule the selected task.
- **View Logs** - opens the **Properties** window, Logs tab, where you can see the reports generated after the selected task was run.
- **Clone Task** - duplicates the selected task. This is useful when creating new tasks, as you can modify the settings of the task duplicate.
- **Delete** - deletes the selected task.

> *Note*
> Available for user-created tasks only. You cannot remove a default task.

- **Properties** - opens the **Properties** window, Overview tab, where you can change the settings of the selected task.

Due to the particular nature of the **Misc Tasks** category, only the **View Logs** and **Properties** options are available in this case.

Configuring Scan Settings

To configure the scanning options of a specific scan task, right-click it and select **Properties**.

You can easily configure the scanning options by adjusting the scan level. Drag the slider along the scale to set the desired scan level. Use the description on the right side of the scale to identify the scan level that better fits your needs.

You can also configure these general options:

- **Run the task with Low priority.** Decreases the priority of the scan process. You will allow other programs to run faster and increase the time needed for the scan process to finish.
- **Minimize Scan Wizard to system tray.** Minimizes the scan window to the system tray. Double-click SHIELD DELUXE 2013 icon to open it.
- Specify the action to be taken if no threats are found.

Advanced users might want to take advantage of the scan settings SHIELD DELUXE 2013 offers. The scanner can be set to scan only specific file extensions, to search for specific malware threats or to skip archives. This may greatly reduce scanning times and improve your computer's responsiveness during a scan.

To configure the scan settings in detail:

1. Click **Custom**.
2. Configure the scan settings as needed. To find out what an option does, keep the mouse over it and read the description displayed at the bottom of the window.
3. Click **OK** to save the changes and close the window.

You may find this information useful:

- If you are not familiar with some of the terms, check them in the glossary. You can also find useful information by searching the Internet.
- **Scan Level.** Specify the type of malware you want SHIELD DELUXE 2013 to scan for by selecting the appropriate options.
- **Scan files.** You can set SHIELD DELUXE 2013 to scan all types of files, applications (program files) only or specific file types you consider to be dangerous. Scanning all files provides best protection, while scanning applications only can be used to perform a quicker scan.

  Applications (or program files) are far more vulnerable to malware attacks than other types of files. This category includes the following file extensions: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml`; `.nws`.

  If you opt for **Scan user defined extensions**, it is recommended that you include all application extensions beside other file extensions you consider to be dangerous.
- **Scan only new and changed files.** By scanning only new and changed files, you may greatly improve overall system responsiveness with a minimum trade-off in security.
- **Scan inside archives.** Archives containing infected files are not an immediate threat to the security of your system. The malware can affect your system only if the infected file is extracted from the archive and executed without having real-time

protection enabled. However, it is recommended to use this option in order to detect and remove any potential threat, even if it is not an immediate threat.

Note
Scanning archived files increases the overall scanning time and requires more system resources.

- **Action options.** Specify the actions to be taken on each category of detected files using the options in this category. There are three categories of detected files:
  - **Infected files.** Files detected as infected match a malware signature in SHIELD DELUXE 2013 Malware Signature Database. SHIELD DELUXE 2013 can normally remove the malware code from an infected file and reconstruct the original file. This operation is known as disinfection.

    Note
    Malware signatures are snippets of code extracted from actual malware samples. They are used by antivirus programs to perform pattern-matching and detect malware.
    SHIELD DELUXE 2013 Malware Signature Database is a collection of malware signatures updated hourly by SHIELD DELUXE 2013 malware researchers.

  - **Suspicious files.** Files are detected as suspicious by the heuristic analysis. Suspicious files cannot be disinfected, because no disinfection routine is available.
  - **Hidden files (rootkits).** Please note that these hidden files are not the files that you deliberately hide from Windows. They are the files hidden by special programs, known as rootkits. Rootkits are not malicious in nature. However, they are commonly used to make viruses or spyware undetectable by normal antivirus programs.

  You should not change the default actions taken on detected files unless you have a strong reason to do so.

  To set a new action, click the current **First action** and select the desired option from the menu. Specify a **Second action** that will be taken in case the first one fails.

Click **OK** to save the changes and close the window. To run the task, just click **Scan**.

Setting Scan Target

You cannot modify the scan target of the scan tasks from the **System Tasks** category. You can only see their scan target. To view the scan target of a specific system scan task, right-click the task and select **Show Scan Paths**.

To set the scan target of a specific user scan task, right-click the task and select **Paths**. Alternatively, if you are already in the Properties window of a task, select the **Paths** tab.

You can see the list of local, network and removable drives as well as the files or folders added previously, if any. All checked items will be scanned when running the task.

The following buttons are available:

- **Add Item(s)** - opens a browsing window where you can select the file(s) / folder(s) that you want to be scanned.

Note
You can also use drag and drop to add files/folders to the list.

- **Delete Item(s)** - removes the file(s) / folder(s) previously selected from the list of objects to be scanned.

Besides these buttons, there are some options that allow the fast selection of the scan locations.

- **Local Drives** - to scan the local drives.
- **Network Drives** - to scan all network drives.
- **Removable Drives** - to scan removable drives (CD-ROM, floppy-disk unit).
- **All Entries** - to scan all drives, no matter if they are local, in the network or removable.

Click **OK** to save the changes and close the window. To run the task, just click **Scan**.

Scheduling Scan Tasks

With complex tasks, the scanning process will take some time and it will work best if you close all other programs. That is why it is best for you to schedule such tasks when you are not using your computer and it has gone into the idle mode.

To see the schedule of a specific task or to modify it, right-click the task and select **Schedule**. If you are already in a task's Properties window, select the **Scheduler** tab.

You can see the task schedule, if any.

When scheduling a task, you must choose one of the following options:

- **No** - launches the task only when the user requests it.
- **Once** - launches the scan only once, at a certain moment. Specify the start date and time in the **Start Date/Time** fields.
- **Periodically** - launches the scan periodically, at certain time intervals(minutes, hours, days, weeks, months) starting with a specified date and time.
- **On system startup** - launches the scan at the specified number of minutes after a user has logged on to Windows.

Click **OK** to save the changes and close the window. To run the task, just click **Scan**.

15.3. Configuring Scan Exclusions

There are cases when you may need to exclude certain files from scanning. For example, you may want to exclude an EICAR test file from on-access scanning or `.avi` files from on-demand scanning.

SHIELD DELUXE 2013 allows excluding objects from on-access or on-demand scanning, or from both. This feature is intended to decrease scanning times and to avoid interference with your work.

Two types of objects can be excluded from scanning:

- **Paths** - the file or the folder (including all the objects it contains) indicated by a specified path will be excluded from scanning.
- **Extensions** - all files having a specific extension will be excluded from scanning, no matter what their location on the hard drive.

The objects excluded from on-access scanning will not be scanned, no matter if they are accessed by you or by an application.

Note

Exclusions will NOT apply for contextual scanning. Contextual scanning is a type of on-demand scanning: you right-click the file or folder you want to scan and select **Scan with SHIELD DELUXE 2013**.

15.3.1. Excluding Files or Folders from Scanning

To exclude paths from scanning:

1. Open SHIELD DELUXE 2013.
2. Depending on the user interface view mode, proceed as follows:

   Intermediate View

   Go to the **Security** tab and click **Configure Antivirus** in the Quick Tasks area on the left side of the window.

   Go to the **Exclusions** tab.

   Expert View

   Go to **Antivirus > Exclusions**.

   > *Note*
   >
   > In Basic View and Intermediate View, you can configure a shortcut so that you can access these settings from your dashboard. For more information, please refer to "*My Tools*" (p. 29).

3. Select the corresponding check box to enable scan exclusions.
4. Start the configuration wizard as follows:
   - Right-click in the Files and Folders table and select **Add new path**.
   - Click the **Add** button, located at the top of the exclusions table.
5. Follow the configuration wizard. You can navigate through the wizard using the **Next** and **Back** buttons. To exit the wizard, click **Cancel**.

   a. Select the option of excluding a path from scanning. This step appears only when you start the wizard by clicking the **Add** button.

   b. To specify the paths to be excluded from scanning use either of the following methods:
      - Click **Browse**, select the file or folder that you want to be excluded from scanning and then click **Add**.
      - Type the path that you want to be excluded from scanning in the edit field and click **Add**.

      The paths will appear in the table as you add them. You can add as many paths as you want.

c. By default, the selected paths are excluded from both on-access and on-demand scanning. To change when to apply the exception, click on the right column and select the desired option from the list.

d. It is highly recommended to scan the files in the specified paths to make sure that they are not infected. Select the check box to scan these files before excluding them from scanning.

   Click **Finish** to add the scan exclusions.

6. Click **Apply** to save the changes.

15.3.2. Excluding File Extensions from Scanning

To exclude file extensions from scanning:

1. Open SHIELD DELUXE 2013.
2. Depending on the user interface view mode, proceed as follows:

   Intermediate View

   Go to the **Security** tab and click **Configure Antivirus** in the Quick Tasks area on the left side of the window.

   Go to the **Exclusions** tab.

   Expert View

   Go to **Antivirus > Exclusions**.

   Note

   In Basic View and Intermediate View, you can configure a shortcut so that you can access these settings from your dashboard. For more information, please refer to "*My Tools*" (p. 29).

3. Select the corresponding check box to enable scan exclusions.
4. Start the configuration wizard as follows:
   - Right-click in the Extensions table and select **Add new extensions**.
   - Click the **Add** button, located at the top of the exclusions table.
5. Follow the configuration wizard. You can navigate through the wizard using the **Next** and **Back** buttons. To exit the wizard, click **Cancel**.

   a. Select the option of excluding extensions from scanning. This step appears only when you start the wizard by clicking the **Add** button.

b. To specify the extensions to be excluded from scanning use either of the following methods:

   - Select from the menu the extension that you want to be excluded from scanning and then click **Add**.

     Note
     The menu contains a list of all the extensions registered on your system. When you select an extension, you can see its description, if available.

   - Type the extension that you want to be excluded from scanning in the edit field and click **Add**.

   The extensions will appear in the table as you add them. You can add as many extensions as you want.

c. By default, the selected extensions are excluded from both on-access and on-demand scanning. To change when to apply the exception, click on the right column and select the desired option from the list.

d. It is highly recommended to scan the files with the specified extensions to make sure that they are not infected.

   Click **Finish** to add the scan exclusions.

6. Click **Apply** to save the changes.

15.3.3. Managing Scan Exclusions

If the configured scan exclusions are no longer needed, it is recommended that you delete them or disable scan exclusions.

To manage scan exclusions:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus > Exclusions**.

To remove an entry from the table, select it and click the **Delete** button.

To edit an entry from the table, select it and click the **Edit** button. A new window will appear where you can change the extension or the path to be excluded and the type of scanning you want them to be excluded from, as needed. Make the necessary changes and click **OK**.

Note
You can also right-click an object and use the options on the shortcut menu to edit or delete it.

To disable scan exclusions, clear the corresponding check box.

15.4. Quarantine Area

SHIELD DELUXE 2013 allows isolating the infected or suspicious files in a secure area, named quarantine. By isolating these files in the quarantine, the risk of getting infected disappears and, at the same time, you have the possibility to send these files for further analysis to SHIELD DELUXE 2013 lab.

Note
When a virus is in quarantine it cannot do any harm because it cannot be executed or read.

In addition, SHIELD DELUXE 2013 scans the quarantined files after each malware signature update. Cleaned files are automatically moved back to their original location.

To see and manage quarantined files and to configure the quarantine settings:

1. Open SHIELD DELUXE 2013.
2. Depending on the user interface view mode, proceed as follows:

   Intermediate View

   Go to the **Security** tab and click **Configure Antivirus** in the Quick Tasks area on the left side of the window.

   Go to the **Quarantine** tab.

   Expert View

   Go to **Antivirus > Quarantine**.

   Note

   In Basic View and Intermediate View, you can configure a shortcut so that you can access these settings from your dashboard. For more information, please refer to "*My Tools*" (p. 29).

Managing Quarantined Files

You can send any selected file from the quarantine to SHIELD DELUXE 2013 Lab by clicking **Send**. By default, SHIELD DELUXE 2013 will automatically submit quarantined files every 60 minutes.

To delete a quarantined file, select it and click the **Delete** button.

If you want to restore a quarantined file to its original location, select it and click **Restore**.

Configuring Quarantine Settings

To configure the quarantine settings, click **Settings**. Using the quarantine settings, you can set SHIELD DELUXE 2013 to automatically perform the following actions:

Delete old files. To automatically delete old quarantined files, check the corresponding option. You must specify the number of days after which the quarantined files should be deleted and frequency with which SHIELD DELUXE 2013 should check for old files.

Automatically submit files. To automatically submit quarantined files, check the corresponding option. You must specify the frequency with which to submit files.

Scan quarantined files after update. To automatically scan quarantined files after each update performed, check the corresponding option. You can choose to automatically move back the cleaned files to their original location by selecting **Restore clean files**.

Click **OK** to save the changes and close the window.

16. Antiphishing Protection

SHIELD DELUXE 2013 Antiphishing prevents you from disclosing personal information while browsing the Internet by alerting you about potential phishing web pages.

SHIELD DELUXE 2013 provides real-time antiphishing protection for:

- Internet Explorer
- Mozilla Firefox
- Yahoo! Messenger
- Windows Live (MSN) Messenger

16.1. Configuring the Antiphishing White List

You can configure and manage a white list of web sites that will not be scanned by SHIELD DELUXE 2013 Antiphishing engines. The white list should contain only web sites you fully trust. For example, add the web sites where you currently shop online.

Note

You can easily add web sites to the white list from SHIELD DELUXE 2013 Antiphishing toolbar integrated into your web browser. For more information, please refer to "*Managing SHIELD DELUXE 2013 Antiphishing Protection in Internet Explorer and Firefox*" (p. 81).

To configure and manage the antiphishing white list:

- If you are using a supported web browser, click SHIELD DELUXE 2013 toolbar and choose **White List** from the menu.
- Alternatively, follow these steps:
  1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
  2. Go to **Antivirus > Shield**.
  3. Click **White List**.

To add a site to the White List, provide its address in the corresponding field and click **Add**.

If you want to remove a web site from the white list, click the corresponding **Remove** button.

Click **Save** to save the changes and close the window.

16.2. Managing SHIELD DELUXE 2013 Antiphishing Protection in Internet Explorer and Firefox

SHIELD DELUXE 2013 integrates directly through an intuitive and easy-to-use toolbar into the following web browsers:

- Internet Explorer
- Mozilla Firefox

You can easily and efficiently manage antiphishing protection and the White List using SHIELD DELUXE 2013 Antiphishing toolbar integrated into one of the above web browsers.

The antiphishing toolbar is located on the topside of browser. Click it in order to open the toolbar menu.

> *Note*
> If you cannot see the toolbar, open the **View** menu, point to **Toolbars** and check **The Shield Deluxe Toolbar**.

The following commands are available on the toolbar menu:

- **Enable / Disable** - enables / disables SHIELD DELUXE 2013 antiphishing protection in the current web browser.
- **Settings** - opens a window where you can specify the antiphishing toolbar's settings. The following options are available:
  - **Real-time Antiphishing Web Protection** - detects and alerts you in real-time if a web site is phished (set up to steal personal information). This option controls SHIELD DELUXE 2013 antiphishing protection in the current web browser only.
  - **Ask before adding to whitelist** - prompts you before adding a web site to the White List.
- **Add to White List** - adds the current web site to the White List.

> *Important*
> Adding a site to the White List means that SHIELD DELUXE 2013 will not scan the site for phishing attempts anymore. We recommend you to add to the White List only sites that you fully trust.

- **White List** - opens the White List. For more information, please refer to *"Configuring the Antiphishing White List"* (p. 80).
- **Report as Phishing** - informs SHIELD DELUXE 2013 Lab that you consider the respective web site to be used for phishing. By reporting phished web sites you help protect other people against identity theft.
- **Help** - opens the help file.
- **About** - opens a window where you can see information about SHIELD DELUXE 2013 and where to look for help in case something unexpected appears.

17. Search Advisor

Search Advisor improves your online threat protection by alerting you about phishing or untrusted web pages directly from your search results page.

Search Advisor works with any web browser and checks the search results displayed by the most popular search engines:

- Google
- Yahoo!
- Bing

Search Advisor indicates whether a search result is safe or not by placing a small status icon before the link.

✓ **Green circle with a check mark:** You can safely access the link.

❗ **Red circle with an exclamation mark:** This is a phishing or untrusted web page. You should avoid opening the link. If you are using Internet Explorer or Firefox and you try to open the link, SHIELD DELUXE 2013 will automatically block the web page and display an alert page instead. If you want to ignore the alert and access the web page, follow the instructions in the alert page.

17.1. Disabling Search Advisor

To disable Search Advisor:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Preferences**.
2. Go to **Security Settings**.
3. Use the switch to turn off Search Advisor.

18. Privacy Control

SHIELD DELUXE 2013 monitors dozens of potential “hotspots” in your system where spyware might act, and also checks any changes made to your system and software. It is effective in blocking Trojan horses and other tools installed by hackers, who try to compromise your privacy and send your personal information, like credit card numbers, from your computer to the hacker.

Privacy Control includes these components:

- Identity Control - helps you make sure that your personal information is not sent from your computer without your consent. It scans the e-mail and instant messages sent from your computer, as well as any data sent via web pages, and blocks any piece of information protected by the Identity Control rules you have created.
- Registry Control - asks for your permission whenever a program tries to modify a registry entry in order to be executed at Windows start-up.
- Cookie Control - asks for your permission whenever a new website tries to set a cookie.
- Script Control - asks for your permission whenever a website tries to activate a script or other active content.

By default, only Identity Control is enabled. You must configure appropriate Identity Control rules to prevent the unauthorized sending of confidential information. For more information, please refer to “*Configuring Identity Control*” (p. 86).

The other components of Privacy Control are interactive. If you enable them, you will be prompted, through alert windows, to allow or block specific actions when you browse new web sites or install new software. This is why they are usually used by advanced users.

18.1. Configuring Protection Level

The protection level helps you easily enable or disable the Privacy Control components.

To configure the protection level:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Privacy Control > Status**.

3. Make sure Privacy Control is enabled.
4. There are two options:
   - Drag the slider along the scale to set the appropriate protection level. Click **Default Level** to position the slider at the default level.

     Use the description on the right side of the scale to choose the protection level that better fits your security needs.
   - You can customize the protection level by clicking **Custom level**. In the window that will appear, select the protection controls you want to enable and click **OK**.

18.2. Identity Control

Identity Control protects you against the theft of sensitive data when you are online.

Consider a simple example: you have created an Identity Control rule that protects your credit card number. If a spyware software somehow manages to install on your computer, it cannot send your credit card number via e-mail, instant messages or web pages. Moreover, your children cannot use it to buy online or reveal it to people they met on the Internet.

To learn more, please refer to these topics:

- "*About Identity Control*" (p. 85).
- "*Configuring Identity Control*" (p. 86).
- "*Managing Rules*" (p. 89).

18.2.1. About Identity Control

Keeping confidential data safe is an important issue that bothers us all. Data theft has kept pace with the development of Internet communications and it makes use of new methods of fooling people into giving away private information.

Whether it is your e-mail or your credit card number, when they fall into the wrong hands such information may cause you damage: you may find yourself drowning in spam messages or you might be surprised to access an emptied account.

Identity Control protects you against the theft of sensitive data when you are online. Based on the rules you create, Identity Control scans the web, e-mail and instant messaging traffic leaving your computer for specific character strings (for example, your credit card number). If there is a match, the respective web page, e-mail or instant message is blocked.

You can create rules to protect any piece of information you might consider personal or confidential, from your phone number or e-mail address to your bank account information. Multiuser support is provided so that users logging on to different Windows user accounts can configure and use their own identity protection rules. If your Windows account is an administrator account, the rules you create can be configured to also apply when other users of the computer are logged on to their Windows user accounts.

Why use Identity Control?

- Identity Control is very effective in blocking keylogger spyware. This type of malicious applications records your keystrokes and sends them over the Internet to a malicious person (hacker). The hacker can find out sensitive information from the stolen data, such as bank account numbers and passwords, and use it to gain personal benefits.

  Supposing such an application manages to avoid antivirus detection, it cannot send the stolen data by e-mail, web or instant messages if you have created appropriate identity protection rules.

- Identity Control can protect you from phishing attempts (attempts to steal personal information). The most common phishing attempts make use of a deceiving e-mail to trick you into submitting personal information on a fake web page.

  For example, you may receive an e-mail claiming to be from your bank and requesting you to urgently update your bank account information. The e-mail provides you with a link to the web page where you must provide your personal information. Although they seem to be legitimate, the e-mail and the web page the misleading link directs you to are fake. If you click the link in the e-mail and submit your personal information on the fake web page, you will disclose this information to the malicious persons who organized the phishing attempt.

  If appropriate identity protection rules are in place, you cannot submit personal information (such as your credit card number) on a web page unless you have explicitly defined an exception for the respective web page.

- Using Identity Control rules, you can prevent your children from giving out personal information (such as the home address or phone number) to people they met on the Internet. Moreover, if you create rules to protect your credit card, they cannot use it to buy things online without your consent.

18.2.2. Configuring Identity Control

If you want to use Identity Control, follow these steps:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Privacy Control > Identity**.
3. Make sure Identity Control is enabled.

   Note
   If the option cannot be configured, go to the **Status** tab and enable Privacy Control.

4. Create rules to protect your sensitive data. For more information, please refer to "*Creating Identity Protection Rules*" (p. 87).
5. If needed, define specific exclusions from the rules you have created. For example, if you have created a rule to protect your credit card number, add the web sites where you usually use your credit card to the exclusions list. For more information, please refer to "*Defining Exclusions*" (p. 88).

Creating Identity Protection Rules

To create an identity protection rule, click the ⊞ **Add** button and follow the configuration wizard. You can navigate through the wizard using the **Next** and **Back** buttons. To exit the wizard, click **Cancel**.

1. **Welcome Window**
2. **Set Rule Type and Data**

   You must set the following parameters:

   - **Rule Name** - type the name of the rule in this edit field.
   - **Rule Type** - choose the rule type (address, name, credit card, PIN, SSN etc).
   - **Rule Data** - type the data you want to protect in this edit field. For example, if you want to protect your credit card number, type all or part of it here.

   Important
   If you enter less than three characters, you will be prompted to validate the data. We recommend you to enter at least three characters in order to avoid the mistaken blocking of messages and web pages.

   All of the data you enter is encrypted. For extra safety, do not enter all of the data you wish to protect.

3. **Select Traffic Types and Users**

   a. Select the type of traffic you want SHIELD DELUXE 2013 to scan.

   - **Scan Web (HTTP traffic)** - scans the HTTP (web) traffic and blocks the outgoing data that matches the rule data.
   - **Scan e-mail (SMTP traffic)** - scans the SMTP (mail) traffic and blocks the outgoing e-mail messages that contain the rule data.
   - **Scan IM (Instant Messaging) traffic** - scans the Instant Messaging traffic and blocks the outgoing chat messages that contain the rule data.

   You can choose to apply the rule only if the rule data matches whole words or if the rule data and the detected string case match.

   b. Specify the users for which the rule applies.

   - **Only for me (current user)** - the rule will apply only to your user account.
   - **Limited user accounts** - the rule will apply to you and all limited Windows accounts.
   - **All users** - the rule will apply to all Windows accounts.

4. **Describe Rule**

   Enter a short description of the rule in the edit field. Since the blocked data (character string) is not displayed in plain text when accessing the rule, the description should help you easily identify it.

   Click **Finish**. The rule will appear in the table.

From now on, any attempt to send the specified data (through e-mail, instant messaging or over a web page) will fail. An alert message will be displayed indicating that SHIELD DELUXE 2013 has blocked identity specific content from being sent.

Defining Exclusions

There are cases when you need to define exceptions to specific identity rules. Let's consider the case when you create a rule that prevents your credit card number from being sent over HTTP (web). Whenever your credit card number is submitted on a website from your user account, the respective page is blocked. If you want, for example, to buy footwear from an online shop (which you know to be secure), you will have to specify an exception to the respective rule.

To open the window where you can manage exceptions, click **Exclusions**.

To add an exception, follow these steps:

1. Click the **Add** button to add a new entry in the table.
2. Double-click **Specify excluded item** and provide the web site, the e-mail address or the IM contact that you want to add as exception.
3. Double-click **Traffic type** and choose from the menu the option corresponding to the type of address previously provided.
   - If you have specified a web address, select **HTTP**.
   - If you have specified an e-mail address, select **E-mail (SMTP)**.
   - If you have specified an IM contact, select **IM**.

To remove an exception from the list, select it and click the **Remove** button.

Click **OK** to save the changes.

18.2.3. Managing Rules

To manage the Identity Control rules:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Privacy Control > Identity**.

You can see the rules created so far listed in the table.

To delete a rule, select it and click the **Delete** button.

To edit a rule select it and click the **Edit** button or double-click it. A new window will appear. Here you can change the name, description and parameters of the rule (type, data and traffic). Click **OK** to save the changes.

18.3. Registry Control

A very important part of the Windows operating system is called the **Registry**. This is where Windows keeps its settings, installed programs, user information and so on.

The **Registry** is also used to define which programs should be launched automatically when Windows is started. Viruses often use this in order to be automatically launched when the user restarts his computer.

Registry Control keeps an eye on the Windows Registry - this is again useful for detecting Trojan horses. It will alert you whenever a program will try to modify a registry entry in order to be executed at Windows start-up. For more information, please refer to "*Registry Alerts*" (p. 35).

To configure Registry Control:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Privacy Control > Registry**.
3. Select the corresponding check box to enable Registry Control.

Note

If the option cannot be configured, go to the **Status** tab and enable Privacy Control.

Managing Rules

To delete a rule, select it and click the **Delete** button.

18.4. Cookie Control

Cookies are a very common occurrence on the Internet. They are small files stored on your computer. Websites create these cookies in order to keep track of specific information about you.

Cookies are generally made to make your life easier. For example they can help the website remember your name and preferences, so that you don't have to enter them on every visit.

But cookies can also be used to compromise your privacy, by tracking your surfing patterns.

This is where Cookie Control helps. When enabled, Cookie Control will prompt you for permission whenever a new web site tries to set or request a cookie. For more information, please refer to "*Cookie Alerts*" (p. 36).

To configure Cookie Control:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Privacy Control > Cookie**.
3. Select the corresponding check box to enable Cookie Control.

Note
If the option cannot be configured, go to the **Status** tab and enable Privacy Control.

4. You can configure rules for the web sites you visit regularly, but it is not really necessary. Rules are automatically created through the alert window, based on your answer.

Note
Because of the great number of cookies used on the Internet today, **Cookie Control** can be quite bothersome to begin with. At first, it will ask a lot of questions about sites trying to place cookies on your computer. As soon as you add your regular sites to the rule-list, surfing will become as easy as before.

Creating Rules Manually

To manually create a rule, click the **Add** button and configure the rule parameters in the configuration window. You can set the parameters:

- **Domain address** - type in the domain on which the rule should apply.
- **Action** - select the action of the rule.

Action	*Description*
Allow	The cookies on that domain will execute.
Deny	The cookies on that domain will not execute.

- **Direction** - select the traffic direction.

Type	*Description*
Outgoing	The rule applies only for the cookies that are sent out back to the connected site.
Incoming	The rule applies only for the cookies that are received from the connected site.
Both	The rule applies in both directions.

Note
You can accept cookies but never return them by setting the action to **Deny** and the direction to **Outgoing**.

Click **Finish**.

Managing Rules

To delete a rule, select it and click the **Delete** button. To modify the rule parameters, select the rule and click the **Edit** button or double-click it. Make the desired changes in the configuration window.

18.5. Script Control

Scripts and other codes such as ActiveX controls and Java applets, which are used to create interactive web pages, can be programmed to have harmful effects. ActiveX elements, for example, can gain total access to your data and they can read data from your computer, delete information, capture passwords and intercept messages while you're online. You should only accept active content from sites you fully know and trust.

If you enable Script Control, you will be prompted for permission whenever a new web site tries to run a script or other active content. For more information, please refer to "*Script Alerts*" (p. 36).

To configure Script Control:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Privacy Control > Script**.
3. Select the corresponding check box to enable Script Control.

> *Note*
> If the option cannot be configured, go to the **Status** tab and enable Privacy Control.

4. You can configure rules for the web sites you visit regularly, but it is not really necessary. Rules are automatically created through the alert window, based on your answer.

Creating Rules Manually

To manually create a rule, click the **Add** button and configure the rule parameters in the configuration window. You can set the parameters:

- **Domain address** - type in the domain on which the rule should apply.
- **Action** - select the action of the rule.

Action	*Description*
Allow	The scripts on that domain will execute.
Deny	The scripts on that domain will not execute.

Click **Finish**.

Managing Rules

To delete a rule, select it and click the **Delete** button. To modify the rule parameters, select the rule and click the **Edit** button or double-click it. Make the desired changes in the configuration window.

19. Vulnerability

An important step in protecting your computer against malicious persons and applications is to keep up to date the operating system and the applications you regularly use. Moreover, to prevent unauthorized physical access to your computer, strong passwords (passwords that cannot be easily guessed) must be configured for each Windows user account.

SHIELD DELUXE 2013 regularly checks your system for vulnerabilities and notifies you about the existing issues.

19.1. Checking for Vulnerabilities

You can check for vulnerabilities and fix them step by step by using the **Vulnerability Scan** wizard. To start the wizard, open SHIELD DELUXE 2013 and, depending on the user interface view mode, proceed as follows:

Intermediate View

Go to the **Security** tab and click **Vulnerability Scan** in the Quick Tasks area on the left side of the window.

Expert View

Go to **Vulnerability > Status** and click **Check Now**.

Follow the six-step guided procedure to remove vulnerabilities from your system. You can navigate through the wizard using the **Next** button. To exit the wizard, click **Cancel**.

1. **Protect your PC**

   Select vulnerabilities to check.

2. **Scan selected issues...**

   Wait for SHIELD DELUXE 2013 to finish checking your system for vulnerabilities.

3. **Windows Updates**

   You can see the list of critical and non-critical Windows updates that are not currently installed on your computer. Select the updates you want to install.

4. **Application Updates**

   If an application is not up to date, click the provided link to download the latest version.

5. **Weak Passwords**

   You can see the list of the Windows user accounts configured on your computer and the level of protection their password provides. Click **Fix** to modify the weak passwords.

6. **Summary**

   This is where you can view the operation result.

19.2. Status

To see the current vulnerability status and enable/disable automatic vulnerability scanning, follow these steps:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Vulnerability > Status**.

The table displays the issues covered in the last vulnerability check and their status. You can see the action you have to take to fix each vulnerability, if any. If the action is **None**, then the respective issue does not represent a vulnerability.

> *Important*
> To be automatically notified about system or application vulnerabilities, keep the **Automatic Vulnerability Scanning** enabled.

Depending on the issue, to fix a specific vulnerability proceed as follows:

- If Windows updates are available, click **Install** in the **Action** column to install them.
- If an application is outdated, click **More info** to view version information and find a link to the vendor web page from where you can install the latest version of that application.
- If a Windows user account has a weak password, click **View & Fix** to force the user to change the password at the next logon or change the password yourself. For a strong password, use a combination of uppercase and lowercase letters, numbers and special characters (such as #, $ or @).
- If the Media Autorun feature is enabled in Windows, click **Fix** to disable it.

19.3. Settings

To configure the settings of the automatic vulnerability checking, follow these steps:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Vulnerability > Settings**.
3. Select the check boxes corresponding to the system vulnerabilities you want to be regularly checked.
   - **Critical Windows Updates**
   - **Regular Windows Updates**
   - **Application Updates**
   - **Weak Passwords**
   - **Media Autorun**

Note

If you clear the check box corresponding to a specific vulnerability, SHIELD DELUXE 2013 will no longer notify you about the related issues.

20. Chat Encryption

The contents of your instant messages should remain between you and your chat partner. By encrypting your conversations, you can make sure anyone trying to intercept them on their way to and from your contacts will not be able to read their contents.

By default, SHIELD DELUXE 2013 encrypts all your instant messaging chat sessions provided that:

- Your chat partner has a PCSecurityShield product installed that supports IM Encryption and IM Encryption is enabled for the instant messaging application used for chatting.
- You and your chat partner use either Yahoo Messenger or Windows Live (MSN) Messenger.

Important
SHIELD DELUXE 2013 will not encrypt a conversation if a chat partner uses a web-based chat application such as Meebo, or if one of the chat partners uses Yahoo! and the other Windows Live (MSN).

To configure instant messaging encryption:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Encryption > Chat Encryption**.

Note
You can easily configure instant messaging encryption for each chat partner using the SHIELD DELUXE 2013 toolbar in the chat window.

By default, IM Encryption is enabled for both Yahoo Messenger and Windows Live (MSN) Messenger. You can choose to disable IM Encryption for a specific chat application only or completely.

Two tables are displayed:

- **Encryption Exclusions** - lists the user IDs and the associated IM program for which encryption is disabled. To remove a contact from the list, select it and click the ⊟ **Remove** button.

- **Current Connections** - lists the current instant messaging connections (user ID and associated IM program) and whether or not they are encrypted. A connection may not be encrypted for these reasons:
  - You explicitly disabled encryption for the respective contact.
  - Your contact does not have installed a PCSecurityShield product that supports IM encryption.

20.1. Disabling Encryption for Specific Users

To disable encryption for a specific user, follow these steps:

1. Click the **Add** button to open the configuration window.
2. Type in the edit field the user ID of your contact.
3. Select the instant messaging application associated with the contact.
4. Click **OK**.

20.2. SHIELD DELUXE 2013 Toolbar in the Chat Window

You can easily configure instant messaging encryption using SHIELD DELUXE 2013 toolbar from the chat window.

The toolbar should be located in the bottom-right corner of the chat window. Look for SHIELD DELUXE 2013 logo to find it.

Note

The toolbar indicates that a conversation is encrypted by displaying a small key 🔑

By clicking SHIELD DELUXE 2013 toolbar you are provided with the following options:

- **Permanently disable encryption for `contact`.**
- **Invite `contact` to use encryption.** To encrypt your conversations, your contact must install SHIELD DELUXE 2013 and use a compatible IM program.

21. Game / Laptop Mode

The Game / Laptop Mode module allows you to configure the special operation modes of SHIELD DELUXE 2013:

- Game Mode temporarily modifies the product settings so as to minimize the resource consumption when you play.
- Laptop Mode prevents scheduled tasks from running when the laptop is running on battery in order to save battery power.
- Silent Mode temporarily modifies the product settings so as to minimize the interruptions when you watch movies or presentations.

21.1. Game Mode

Game Mode temporarily modifies protection settings so as to minimize their impact on system performance. While in Game Mode, the following settings are applied:

- All SHIELD DELUXE 2013 alerts and pop-ups are disabled.
- SHIELD DELUXE 2013 real-time protection level is set to **Permissive**.
- Updates are not performed by default.

Note
To change this setting, go to Update>Settings and clear the **Don't update if Game Mode is on** check box.

By default, SHIELD DELUXE 2013 automatically enters Game Mode when you start a game from SHIELD DELUXE 2013's list of known games or when an application goes to full screen. You can manually enter Game Mode using the default `Ctrl+Alt+Shift+G` hotkey. It is strongly recommended that you exit Game Mode when you finished playing (you can use the same default `Ctrl+Alt+Shift+G` hotkey).

Note
While in Game Mode, you can see the letter `G` over the SHIELD DELUXE 2013 icon.

To configure Game Mode:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Game/Laptop Mode > Game Mode**.

At the top of the section, you can see the status of the Game Mode. You can click **Game Mode is enabled** or **Game Mode is turned off** to change the current status.

21.1.1. Configuring Automatic Game Mode

Automatic Game Mode allows SHIELD DELUXE 2013 to automatically enter Game Mode when a game is detected. You can configure the following options:

- **Use the default list of games provided by SHIELD DELUXE 2013** - to automatically enter Game Mode when you start a game from SHIELD DELUXE 2013's list of known games. To view this list, click **Manage Games** and then **Games List**.
- **Full screen action** - you can choose to automatically enter Game Mode or Silent Mode when an application goes to full screen.
- **Ask if the full screen application should be added to the game list** - to be prompted to add a new application to the game list when you leave full screen. By adding a new application to the game list, the next time you start it SHIELD DELUXE 2013 will automatically enter Game Mode.

Note

If you do not want SHIELD DELUXE 2013 to automatically enter Game Mode, clear the **Automatic Game Mode is enabled** check box.

21.1.2. Managing the Game List

SHIELD DELUXE 2013 automatically enters Game Mode when you start an application from the game list. To view and manage the game list, click **Manage Games**. A new window will appear.

New applications are automatically added to the list when:

- You start a game from SHIELD DELUXE 2013's list of known games. To view this list, click **Games List**.
- After leaving full screen, you add the application to the game list from the prompt window.

If you want to disable Automatic Game Mode for a specific application from the list, clear its corresponding check box. You should disable Automatic Game Mode for regular applications that go to full screen, such as web browsers and movie players.

To manage the game list, you can use the buttons placed at the top of the table:

- **Add** - add a new application to the game list.
- **Remove** - remove an application from the game list.
- **Edit** - edit an existing entry in the game list.

21.1.3. Adding or Editing Games

When you add or edit an entry from the game list, a new window will appear.

Click **Browse** to select the application or type the full path to the application in the edit field.

If you do not want to automatically enter Game Mode when the selected application is started, select **Disable**.

Click **OK** to add the entry to the game list.

21.1.4. Configuring Game Mode Settings

To configure the behaviour on scheduled tasks, use these options:

- **Enable this module to modify Antivirus scan tasks schedules** - to prevent scheduled scan tasks from running while in Game Mode. You can choose one of the following options:

Option **Skip**	*Description*
Task Postpone	Do not run the scheduled task at all.
Task	Run the scheduled task immediately after you exit Game Mode.

21.1.5. Changing Game Mode Hotkey

You can manually enter Game Mode using the default `Ctrl+Alt+Shift+G` hotkey. If you want to change the hotkey, follow these steps:

1. Click **Advanced Settings**. A new window will appear.
2. Under the **Use HotKey** option, set the desired hotkey:
   - Choose the modifier keys you want to use by checking one the following: Control key (`Ctrl`), Shift key (`Shift`) or Alternate key (`Alt`).
   - In the edit field, type the letter corresponding to the regular key you want to use.

   For example, if you want to use the `Ctrl+Alt+D` hotkey, you must check only `Ctrl` and `Alt` and type `D`.

   Note
   Removing the check mark next to **Use HotKey** will disable the hotkey.

3. Click **OK** to save the changes.

21.2. Laptop Mode

Laptop Mode is especially designed for laptop and notebook users. Its purpose is to minimize SHIELD DELUXE 2013's impact on power consumption while these devices are running on battery.

While in Laptop Mode, scheduled tasks are by default not performed.

SHIELD DELUXE 2013 detects when your laptop has switched to battery power and it automatically enters Laptop Mode. Likewise, SHIELD DELUXE 2013 automatically exits Laptop Mode, when it detects the laptop is no longer running on battery.

To configure Laptop Mode:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Game/Laptop Mode > Laptop Mode**.

You can see whether Laptop Mode is enabled or not. If Laptop Mode is enabled, The Shield Deluxe will apply the configured settings while the laptop is running on battery.

21.2.1. Configuring Laptop Mode Settings

To configure the behaviour on scheduled tasks, use these options:

- **Enable this module to modify Antivirus scan tasks schedules** - to prevent scheduled scan tasks from running while in Laptop Mode. You can choose one of the following options:

Option Skip	*Description*
Task Postpone	Do not run the scheduled task at all.
Task	Run the scheduled task immediately after you exit Laptop Mode.

21.3. Silent Mode

Silent Mode temporarily modifies protection settings so as to minimize their impact on system performance. While in Silent Mode the following settings are applied:

- All SHIELD DELUXE 2013 alerts and pop-ups are disabled.
- Scheduled scan tasks are by default disabled.

By default, SHIELD DELUXE 2013 automatically enters Silent Mode when you watch a movie or a presentation or when an application goes to full screen. It is strongly recommended that you exit Silent Mode when you finished watching the movie or the presentation.

> *Note*
> While in Silent Mode, you can see a slight modification of the little SHIELD DELUXE 2013 icon located next to your computer clock.

To configure Silent Mode:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Game/Laptop Mode > Silent Mode**.

At the top of the section, you can see the status of the Silent Mode. You can click **Silent Mode is enabled** or **Silent Mode is disabled** to change the current status.

21.3.1. Configuring Full Screen Action

You can configure the following options:

- **Full screen action** - you can choose to automatically enter Game Mode or Silent Mode when an application goes to full screen.

Note
If you do not want SHIELD DELUXE 2013 to automatically enter Silent Mode, clear the **Full Screen Action** check box.

21.3.2. Configuring Silent Mode Settings

To configure the behaviour on scheduled tasks, use these options:

- **Enable this module to modify Antivirus scan tasks schedules** - to prevent scheduled scan tasks from running while in Silent Mode. You can choose one of the following options:

Option **Skip**	*Description*
Task Postpone	Do not run the scheduled task at all.
Task	Run the scheduled task immediately after you exit Silent Mode.

22. Home Network

The Network module allows you to manage SHIELD DELUXE 2013 products installed on your home computers from a single computer. To access the Home Network module, open SHIELD DELUXE 2013 and, depending on the user interface view mode, proceed as follows:

Intermediate View
Go to the **Network** tab.

Expert View
Go to **Home Network**.

Note
You can also add a shortcut to My Tools.

To be able to manage SHIELD DELUXE 2013 products installed on your home computers, you must follow these steps:

1. Enable SHIELD DELUXE 2013 home network on your computer. Set your computer as Server.
2. Go to each computer you want to manage and join the network (set the password). Set each computer as Regular.
3. Go back to your computer and add the computers you want to manage.

22.1. Enabling SHIELD DELUXE 2013 Network

To enable SHIELD DELUXE 2013 home network, follow these steps:

1. Click **Enable Network**. You will be prompted to configure the home management password.
2. Type the same password in each of the edit fields.
3. Set the role of the computer in SHIELD DELUXE 2013 home network:
   - **Server Computer** - select this option on the computer that will be used to manage all the other ones.
   - **Regular Computer** - select this option on the computers that will be managed by the Server Computer.

4. Click **OK**.

You can see the computer name appearing in the network map.

The **Disable Network** button appears.

22.2. Adding Computers to SHIELD DELUXE 2013 Network

Any computer will be automatically added to the network if it meets the following criteria:

- SHIELD DELUXE 2013 home network was enabled on it.
- the role was set to Regular Computer.
- the password set when enabling the network is the same as the password set on the Server Computer.

> *Note*
> In Expert View, you can scan the home network for computers meeting the criteria at any time by clicking the **Auto discover** button.

To manually add a computer to SHIELD DELUXE 2013 home network from the Server Computer, follow these steps:

1. Click **Add Computer**.
2. Type the home management password and click **OK**. A new window will appear.

   You can see the list of computers in the network. The icon meaning is as follows:

   Indicates an online computer with no SHIELD DELUXE 2013 products installed. Indicates an online computer with SHIELD DELUXE 2013 installed.
   Indicates an offline computer with SHIELD DELUXE 2013 installed.
3. Do one of the following:
   - Select from the list the name of the computer to add.
   - Type the IP address or the name of the computer to add in the corresponding field.
4. Click **Add**. You will be prompted to enter the home management password of the respective computer.

5. Type the home management password configured on the respective computer.
6. Click **OK**. If you have provided the correct password, the selected computer name will appear in the network map.

22.3. Managing SHIELD DELUXE 2013 Network

Once you have successfully created a SHIELD DELUXE 2013 home network, you can manage all SHIELD DELUXE 2013 products from a single computer.

If you move the mouse cursor over a computer from the network map, you can see brief information about it (name, IP address, number of issues affecting the system security, SHIELD DELUXE 2013 registration status).

If you click a computer name in the network map, you can see all the administrative tasks you can run on the remote computer.

- **Register SHIELD DELUXE 2013 on this computer**

  Allows you to register SHIELD DELUXE 2013 on this computer by entering a license key.

- **Set a settings password on a remote PC**

  Allows you to create a password to restrict access to SHIELD DELUXE 2013 settings on this PC.

- **Run an on-demand scan task**

  Allows you to run an on-demand scan on the remote computer. You can perform any of the following scan tasks: My Documents Scan, System Scan or Deep System Scan.

- **Fix all issues on this PC**

  Allows you to fix the issues that are affecting the security of this computer by following the Fix All Issues wizard.

- **View History/Events**

  Allows you access to the **History&Events** module of SHIELD DELUXE 2013 product installed on this computer.

- **Update Now**

  Intitiates the Update process for SHIELD DELUXE 2013 product installed on this computer.

- **Set as Update Server for this network**

Allows you to set this computer as update server for all SHIELD DELUXE 2013 products installed on the computers in this network. Using this option will reduce internet traffic, because only one computer in the network will connect to the internet to download updates.

- **Remove PC from home network**

  Allows you to remove a PC from the network.

When SHIELD DELUXE 2013 interface is in Intermediate View, you can run several tasks on all managed computers at the same time by clicking the corresponding buttons.

- **Scan All** - allows you to scan all managed computers at the same time.
- **Update All** allows you to update all managed computers at the same time.
- **Register All** allows you to register all managed computers at the same time.

Before running a task on a specific computer, you will be prompted to provide the local home management password. Type the home management password and click **OK**.

Note

If you plan to run several tasks, you might want to select **Don't show this message again this session**. By selecting this option, you will not be prompted again for this password during the current session.

23. Update

New malware is found and identified every day. This is why it is very important to keep SHIELD DELUXE 2013 up to date with the latest malware signatures.

If you are connected to the Internet through broadband or DSL, SHIELD DELUXE 2013 takes care of this itself. By default, it checks for updates when you turn on your computer and every **hour** after that.

If an update is detected, you may be asked to confirm the update or the update is performed automatically, depending on the automatic update settings.

The update process is performed on the fly, meaning that the files to be updated are replaced progressively. In this way, the update process will not affect product operation and, at the same time, any vulnerability will be excluded.

Important
To be protected against the latest threats keep the **Automatic Update** enabled.

Updates come in the following ways:

- **Updates for the antivirus engines** - as new threats appear, the files containing virus signatures must be updated to ensure permanent up-to-date protection against them. This update type is also known as **Virus Definitions Update**.
- **Updates for the antispyware engines** - new spyware signatures will be added to the database. This update type is also known as **Antispyware Update**.
- **Product upgrades** - when a new product version is released, new features and scan techniques are introduced to the effect of improving the product's performance. This update type is also known as **Product Update**.

23.1. Performing an Update

The automatic update can be done anytime you want by clicking **Update Now**. This update is also known as **Update by user request**.

To update SHIELD DELUXE 2013, depending on the user interface mode, proceed as follows:

Basic View
Click the **Update Now** icon in the Protect your PC area.

Intermediate View

Go to the **Security** tab and click **Update Now** in the Quick Tasks area on the left side of the window.

Expert View

Go to **Update > Update**.

The **Update** module will connect to SHIELD DELUXE 2013 update server and will verify if any update is available. If an update was detected, depending on the options set in the Manual Update Settings section, you will be asked to confirm the update or the update will be made automatically.

Important

It may be necessary to restart the computer when you have completed the update. We recommend doing it as soon as possible.

Note

If you are connected to the Internet through a dial-up connection, then it is recommended to regularly update SHIELD DELUXE 2013 by user request. For more information, please refer to "*How to Update SHIELD DELUXE 2013 on a Slow Internet Connection*" (p. 127).

23.2. Configuring Update Settings

The updates can be performed from the local network, over the Internet, directly or through a proxy server. By default, SHIELD DELUXE 2013 will check for updates every hour, over the Internet, and install the available updates without alerting you.

To configure the update settings:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Update > Settings**.
3. Configure the settings as needed. To find out what an option does, keep the mouse over it and read the description displayed at the bottom of the window.
4. Click **Apply** to save the changes.

To apply the default settings, click **Default**.

The update settings are grouped into 4 categories (**Update Location Settings**, **Automatic Update Settings**, **Manual Update Settings** and **Advanced Settings**). Each category will be described separately.

23.2.1. Setting Update Locations

To set the update locations, use the options from the **Update Location Settings** category.

Note
Configure these settings only if you are connected to a local network that stores SHIELD DELUXE 2013 malware signatures locally or if you connect to the Internet through a proxy server.

For more reliable and faster updates, you can configure a **primary update location** and an **alternate update location**. Change the default settings only when instructed by a representative of PCSecurityShield.

To modify one of the update locations, provide the URL of the local mirror in the **URL** field corresponding to the location you want to change.

If you have configured a SHIELD DELUXE 2013 home network and set one of the computers as Update server, the IP address of that computer is set as primary update location.

Note
We recommend you to set as primary update location the local mirror and to leave the alternate update location unchanged, as a fail-safe plan in case the local mirror becomes unavailable.

In case the company uses a proxy server to connect to the Internet, check **Use proxy** and then click **Proxy Settings** to configure the proxy settings. For more information, please refer to “Connection Settings” (p. 50)

23.2.2. Configuring Automatic Update

To configure the update process performed automatically by SHIELD DELUXE 2013, use the options in the **Automatic Update Settings** category.

You can specify the number of hours between two consecutive checks for updates in the **Update every** field. By default, the update time interval is set to 1 hour.

To specify how the automatic update process should be performed, select one of the following options:

- **Silent update** - SHIELD DELUXE 2013 automatically downloads and implements the update.
- **Prompt before downloading updates** - every time an update is available, you will be prompted before downloading it.

- **Prompt before installing updates** - every time an update was downloaded, you will be prompted before installing it.

23.2.3. Configuring Manual Update

To specify how the manual update (update by user request) should be performed, select one of the following options in the **Manual Update Settings** category:

- **Silent update** - the manual update will be performed automatically in the background, without user intervention.
- **Prompt before downloading updates** - every time an update is available, you will be prompted before downloading it.

23.2.4. Configuring Advanced Settings

To prevent SHIELD DELUXE 2013 update process from interfering with your work, configure the options in the **Advanced Settings** category:

- **Wait for reboot, instead of prompting** - If an update requires a reboot, the product will keep working with the old files until the system is rebooting. The user will not be prompted for rebooting, therefore SHIELD DELUXE 2013 update process will not interfere with the user’s work.
- **Do not update if a scan is in progress** - SHIELD DELUXE 2013 will not update if a scan process is running. This way, SHIELD DELUXE 2013 update process will not interfere with the scan tasks.

> *Note*
>
> If SHIELD DELUXE 2013 is updated while a scan is in progress, the scan process will be aborted.

- **Do not update if Game Mode is on** - SHIELD DELUXE 2013 will not update if the Game Mode is turned on. In this way, you can minimize the product’s influence on system performance during games.
- **Enable update sharing** - If you want to minimize the influence of the network traffic on system performance during updates, use the update sharing option.
- **Upload SHIELD DELUXE 2013 files from this PC** - SHIELD DELUXE 2013 lets you share the latest antivirus signatures available on your PC with other SHIELD DELUXE 2013 users.

How To

24. How Do I Scan Files and Folders?

Scanning is easy and flexible with SHIELD DELUXE 2013. There are several ways to set
SHIELD DELUXE 2013 to scan files and folders for viruses and other malware:

- Using Windows Contextual Menu
- Using Scan Tasks
- Using Scan Activity Bar

Once you initiate a scan, the Antivirus Scan wizard will appear and guide you through the process. For detailed information about this wizard, please refer to "*Antivirus Scan Wizard*" (p. 64).

24.1. Using Windows Contextual Menu

This is the easiest and recommended way to scan a file or folder on your computer. Right-click the object you want to scan and select **Scan with SHIELD DELUXE 2013** from the menu. Follow the Antivirus Scan wizard to complete the scan.

Typical situations when you would use this scanning method include the following:

- You suspect a specific file or folder to be infected.
- Whenever you download from the Internet files that you think they might be dangerous.
- Scan a network share before copying files to your computer.

24.2. Using Scan Tasks

If you want to scan your computer or specific folders regularly, you should consider using scan tasks. Scan tasks instruct SHIELD DELUXE 2013 what locations to scan, and which scanning options and actions to apply. Moreover, you can schedule them to run on a regular basis or at a specific time.

To scan your computer using scan tasks, you must open SHIELD DELUXE 2013 interface and run the desired scan task. Depending on the user interface view mode, different steps are to be followed to run the scan task.

Running Scan Tasks in Basic View

In Basic View, you can run a number of pre-configured scan tasks. Click the **Security** button and choose the desired scan task. Follow the Antivirus Scan wizard to complete the scan.

Running Scan Tasks in Intermediate View

In Intermediate View, you can run a number of pre-configured scan tasks. You can also configure and run custom scan tasks to scan specific locations on your computer using custom scanning options. Follow these steps to run a scan task in Intermediate View:

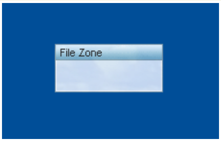
1. Click the **Security** tab.
2. On the left-side Quick Tasks area, click **Full System Scan** and choose the desired scan task. To configure and run a custom scan, click **Custom Scan**.
3. Follow the Antivirus Scan wizard to complete the scan. If you chose to run a custom scan, you must first complete the Custom Scan wizard.

Running Scan Tasks in Expert View

In Expert View, you can run all of the pre-configured scan tasks, and also change their scanning options. Moreover, you can create customized scan tasks if you want to scan specific locations on your computer. Follow these steps to run a scan task in Expert View:

1. Click **Antivirus** on the left-side menu.
2. Click the **Virus Scan** tab. Here you can find a number of default scan tasks and you can create your own scan tasks.
3. Double-click the scan task you want to run.
4. Follow the Antivirus Scan wizard to complete the scan.

24.3. Using Scan Activity Bar



Scan Activity Bar

The **Scan activity bar** is a graphic visualization of the scanning activity on your system. This small window is by default available only in Expert View.

You can use the Scan activity bar to quickly scan files and folders. Drag & drop the file or folder you want to be scanned onto the Scan activity bar. Follow the Antivirus Scan wizard to complete the scan.

Note
For more information, please refer to "*Scan Activity Bar*" (p. 18).

25. How Do I Create a Custom Scan Task?

To create a scan task, open SHIELD DELUXE 2013 and depending on the user interface view mode, proceed as follows:

Intermediate View

Go to the **Security** tab and click **Custom Scan** in the Quick Tasks area on the left side of the window.

A wizard will appear to help you create a scan task. You can navigate through the wizard using the **Next** and **Back** buttons. To exit the wizard, click **Cancel**.

1. **Welcome**
2. **Choose Target**

   Click **Add Target** to select the files or folders to be scanned.

   Click **Advanced Settings**. In the **Overview** tab, adjust the scanning options by moving the cursor on the slider. If you want to configure the scanning options in detail, click **Custom**. Go to the **Scheduler** tab to select when the task will run.
3. **Finish**

   This is where you can enter the task name and optionally add the scan to the Quick Tasks area.

   Click **Start Scan** to create the task and launch the scan wizard.

Expert View

1. Go to **Antivirus > Virus Scan**.
2. Click **New Task**. A new window will appear.

   Note

   You can also right-click a pre-defined scan task, such as **Deep System Scan** and choose **Clone Task**. This is useful when creating new tasks, as you can modify the settings of the task you have duplicated.
3. In the **Overview** tab, enter the task name and adjust the scanning options by moving the cursor on the slider.

   If you want to configure the scanning options in detail, click **Custom**.

4. Go to the **Paths** tab to select the scan target. Click **Add Item(s)** to select the files or folders to be scanned.
5. Go to the **Scheduler** tab to select when the task will run.
6. Click **Ok** to save the task. The new task will appear under the User defined tasks and can be edited, removed or run at any moment from this window.

26. How Do I Schedule a Computer Scan?

Scanning your computer periodically is a best practice to keep your computer free from malware. SHIELD DELUXE 2013 allows you to schedule scan tasks so that you can automatically scan your computer.

To schedule SHIELD DELUXE 2013 to scan your computer, follow these steps:

1. Open SHIELD DELUXE 2013.
2. Depending on the user interface view mode, proceed as follows:

   Intermediate View

   Go to the **Security** tab and click **Configure Antivirus** in the Quick Tasks area on the left side of the window.

   Expert View

   Click **Antivirus** on the left-side menu.
3. Click the **Virus Scan** tab. Here you can find a number of default scan tasks and you can create your own scan tasks.
   - System tasks are available and can run on every Windows user account.
   - User tasks are only available to and can only be run by the user who created them.

   These are the default scan tasks that you can schedule:

   Full System Scan

   Scans the entire system, except for archives. In the default configuration, it scans for all types of malware other than rootkits.

   Quick Scan

   Quick Scan uses in-the-cloud scanning to detect malware running in your system. Running a Quick Scan usually takes less than a minute and uses a fraction of the system resources needed by a regular virus scan.

   Auto-logon Scan

   Scans the items that are run when a user logs on to Windows. To use this task, you must schedule it to run at system startup. By default, the autologon scan is disabled.

Deep System Scan

Scans the entire system. In the default configuration, it scans for all types of malware threatening your system's security, such as viruses, spyware, adware, rootkits and others.

My Documents

Use this task to scan important current user folders: `My Documents`, `Desktop` and `StartUp`. This will ensure the safety of your documents, a safe workspace and clean applications running at startup.

If none of these scan tasks suit your needs, you can create a new scan task, which you can then schedule to run as needed.

4. Right-click the desired scan task and select **Schedule**. A new window will appear.
5. Schedule the task to run as needed:

- To run the scan task one-time only, select **Once** and specify the start date and time.
- To run the scan task after the system startup, select **On system startup**. You can specify how long after the startup the task should start running (in minutes).
- To run the scan task on a regular basis, select **Periodically** and specify the frequency and the start date and time.

Note

For example, to scan your computer every Saturday at 2 AM, you must configure the schedule as follows:

a. Select **Periodically**.

b. In the **At every** field, type 1 and then select **weeks** from the menu. In this way, the task is run once every week.

c. Set as start date the first Saturday to come.

d. Set as start time `2:00:00 AM`.

6. Click **OK** to save the schedule. The scan task will run automatically according to the schedule you have defined. If the computer is shut down when the schedule is due, the task will run the next time you start your computer.

27. How Do I Update SHIELD DELUXE 2013 Using a Proxy Server?

Normally, SHIELD DELUXE 2013 automatically detects and imports the proxy settings from your system. If you connect to the Internet through a proxy server, you may need to find the proxy settings and configure SHIELD DELUXE 2013 accordingly. To find out how to do this, please refer to "*How Do I Find Out My Proxy Settings?*" (p. 140).

After finding the proxy settings, follow these steps:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **General > Settings**.
3. Click **Proxy Settings** from **Connection Settings**.
4. Enter the proxy settings in the corresponding fields.
5. Click **OK**.

If this information was not helpful, you can contact us for support as described in section "*Support*" (p. 137).

Troubleshooting and Getting Help

28. Troubleshooting

This chapter presents some problems you may encounter when using SHIELD DELUXE 2013 and provides you with possible solutions to these problems. Most of these problems can be solved through the appropriate configuration of the product settings.

If you cannot find your problem here, or if the presented solutions do not solve it, you can contact the PCSecurityShield technical support representatives as presented in chapter "*Support*" (p. 137).

28.1. Installation Problems

This article helps you troubleshoot the most common installation problems with The Shield Deluxe. These problems can be grouped into the following categories:

- Installation validation errors: the setup wizard cannot be run due to specific conditions on your system.
- Failed installations: you initiated installation from the setup wizard, but it was not completed successfully.

28.1.1. Installation Validation Errors

When you start the setup wizard, a number of conditions are verified to validate if the installation can be initiated. The following are the most common installation validation errors and solutions to overcome them.

You do not have sufficient privileges to install the program.

In order to run the setup wizard and install SHIELD DELUXE 2013 you need administrator privileges. Do any of the following:

- Log on to a Windows administrator account and run the setup wizard again.
- Right-click the installation file and select **Run as**. Type the user name and password of a Windows administrator account on the system.

The installer has detected a previous SHIELD DELUXE 2013 version that was not uninstalled properly.

SHIELD DELUXE 2013 was previously installed on your system, but the installation was not completely removed. This condition blocks a new installation of SHIELD DELUXE 2013.

To overcome this error and install SHIELD DELUXE 2013, follow these steps:

1. Contact the PCSecurityShield technical support as described in "*Support*" (p. 137) and ask for the uninstall tool.
2. Run the uninstall tool using administrator privileges.
3. Restart your computer.
4. Start the setup wizard again to install SHIELD DELUXE 2013.

SHIELD DELUXE 2013 product is not compatible with your operating system.

You are trying to install SHIELD DELUXE 2013 on an unsupported operating system. Please check the "*System Requirements*" (p. 2) to find out the operating systems you can install SHIELD DELUXE 2013 on.

If your operating system is Windows XP with Service Pack 1 or without any service pack, you can install Service Pack 2 or higher and then run the setup wizard again.

The installation file is designed for a different type of processor.

If you get such an error, you are trying to run an incorrect version of the installation file. There are two versions of SHIELD DELUXE 2013 installation file: one for 32-bit processors and the other for 64-bit processors.

To make sure you have the correct version for your system, download the installation file directly from http://www.PCSecurityShield.com/.

28.1.2. Failed Installation

There are several installation fail possibilities:

- During installation, an error screen appears. You may be prompted to cancel the installation or a button may be provided to run an uninstall tool that will clean up the system.

Note

Immediately after you initiate installation, you may be notified that there is not enough free disk space to install SHIELD DELUXE 2013. In such case, free the required amount of disk space on the partition where you want to install SHIELD DELUXE 2013 and then resume or reinitiate the installation.

- The installation hangs out and, possibly, your system freezes. Only a restart restores system responsiveness.
- Installation was completed, but you cannot use some or all of SHIELD DELUXE 2013 functions.

To troubleshoot a failed installation and install SHIELD DELUXE 2013, follow these steps:

1. **Clean up the system after the failed installation.** If the installation fails, some SHIELD DELUXE 2013 registry keys and files may remain in your system. Such remainders may prevent a new installation of SHIELD DELUXE 2013. They may also affect system performance and stability. This is why you must remove them before you try to install the product again.

   If the error screen provides a button to run an uninstall tool, click that button to clean up the system. Otherwise, proceed as follows:

   a. Contact the PCSecurityShield technical support as described in "*Support*" (p. 137) and ask for the uninstall tool.

   b. Run the uninstall tool using administrator privileges.

   c. Restart your computer.

2. Check if you have any other security solution installed as they may disrupt the normal operation of SHIELD DELUXE 2013. If this is the case, we recommend you to remove all of the other security solutions and then reinstall SHIELD DELUXE 2013.

3. Try again to install SHIELD DELUXE 2013. It is recommended that you download and run the latest version of the installation file from http://www.PCSecurityShield.com/.

4. If installation fails again, contact us for support as described in "*Support*" (p. 137).

28.2. My System Appears to Be Slow

Usually, after installing a security software, there may appear a slight slowdown of the system, which to a certain degree is normal.

If you notice a significant slow down, this issue can appear for the following reasons:

- **SHIELD DELUXE 2013 is not the only security program installed on the system.**

  Though SHIELD DELUXE 2013 searches and removes the security programs found during the installation, it is recommended to remove any other antivirus program you may use before installing SHIELD DELUXE 2013. For more information, please refer to "*How Do I Remove Other Security Solutions?*" (p. 138).

- **The Minimal System Requirements for running SHIELD DELUXE 2013 are not met.**

  If your machine does not meet the Minimal System Requirements, the computer will become sluggish, especially when multiple applications are running at the same time. For more information, please refer to "*Minimal System Requirements*" (p. 2).

- **Your hard disk drives are too fragmented.**

  File fragmentation slows down file access and decreases system performance.

  To defragment your disk using your Windows operating system, follow the path from the Windows start menu: **Start** → **All Programs** → **Accessories** → **System Tools** → **Disk Defragmenter**.

28.3. Scan Doesn't Start

This type of issue can have two main causes:

- **A previous SHIELD DELUXE 2013 installation which was not completely removed or a faulty SHIELD DELUXE 2013 installation**.

  If this is the case, the easiest solution to follow is to remove SHIELD DELUXE 2013 completely from the system and then reinstall it. For more information, please refer to "*How Do I Remove SHIELD DELUXE 2013 Completely?*" (p. 140).

- **SHIELD DELUXE 2013 is not the only security solution installed on your**

  system. In this case, follow these steps:

  1. Remove the other security solution. For more information, please refer to "*How Do I Remove Other Security Solutions?*" (p. 138).

  2. Remove SHIELD DELUXE 2013 completely from the system.

  3. Reinstall SHIELD DELUXE 2013 on the system.

If this information was not helpful, you can contact us for support as described in section "*Support*" (p. 137).

28.4. I Can no Longer Use an Application

This issue occurs when you are trying to use a program which was working normally before installing SHIELD DELUXE 2013.

You may encounter one of these situations:

- You could receive a message from SHIELD DELUXE 2013 that the program is trying to make a modification to the system.
- You could receive an error message from the program you're trying to use.

This type of situation occurs when the Active Virus Control module mistakenly detects some applications as malicious.

Active Virus Control is a SHIELD DELUXE 2013 module which constantly monitors the applications running on your system and reports those with potentially malicious behavior. Since this feature is based on a heuristic system, there may be cases when legitimate applications are reported by Active Virus Control.

When this situation occurs, you can exclude the respective application from being monitored by Active Virus Control.

To add the program to the exclusions list, follow these steps:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus > Shield**.
3. Click **Advanced Settings**.
4. In the new window go to the **Exclusions** tab, click the **Add** button and browse to the location of the program's .exe file (usually located in the `C:\Program Files`).
5. Click **OK** to save the changes and close the window.
6. Close SHIELD DELUXE 2013 window and check if the issue still occurs.

If this information was not helpful, you can contact us for support as described in section "*Support*" (p. 137).

28.5. How to Update SHIELD DELUXE 2013 on a Slow Internet Connection

If you have a slow Internet connection (such as dial-up), errors may occur during the update process.

To keep your system up to date with the latest SHIELD DELUXE 2013 malware signatures, follow these steps:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Update > Settings**.
3. Under **Manual Update Settings**, select **Prompt before downloading updates**.

4. Click **Apply** and go to the **Update** tab.
5. Click **Update Now** and you will see that a new window will appear.
6. Select only **Signatures updates** and then click **Ok**.
7. SHIELD DELUXE 2013 will download and install only the malware signature updates.

28.6. SHIELD DELUXE 2013 Services Are Not Responding

This article helps you troubleshoot SHIELD DELUXE *2013 Services are not responding* error. You may encounter this error as follows:

- SHIELD DELUXE 2013 icon in the system tray is grayed out and a pop-up informs you that SHIELD DELUXE 2013 services are not responding.
- SHIELD DELUXE 2013 window indicates that SHIELD DELUXE 2013 services are not responding.

The error may be caused by one of the following conditions:

- an important update is being installed.
- temporary communication errors between SHIELD DELUXE 2013 services.
- some of SHIELD DELUXE 2013 services are stopped.
- other security solutions running on your computer at the same time with The Shield Deluxe.
- viruses on your system affect the normal operation of SHIELD DELUXE

2013. To troubleshoot this error, try these solutions:

1. Wait a few moments and see if anything changes. The error may be temporary.
2. Restart the computer and wait a few moments until SHIELD DELUXE 2013 is loaded. Open SHIELD DELUXE 2013 to see if the error persists. Restarting the computer usually solves the problem.
3. Check if you have any other security solution installed as they may disrupt the normal operation of SHIELD DELUXE 2013. If this is the case, we recommend you to remove all of the other security solutions and then reinstall SHIELD DELUXE 2013.

4. If the error persists, there may be a more serious problem (for example, you may be infected with a virus that interferes with SHIELD DELUXE 2013). Please contact us for support as described in section "*Support*" (p. 137).

28.7. SHIELD DELUXE 2013 Removal Failed

This article helps you troubleshoot errors that may occur when removing The Shield Deluxe. There are two possible situations:

- During removal, an error screen appears. The screen provides a button to run an uninstall tool that will clean up the system.
- The removal hangs out and, possibly, your system freezes. Click **Cancel** to abort the removal. If this does not work, restart the system.

If removal fails, some SHIELD DELUXE 2013 registry keys and files may remain in your system. Such remainders may prevent a new installation of SHIELD DELUXE 2013. They may also affect system performance and stability. In order to completely remove SHIELD DELUXE 2013 from your system, you must run the uninstall tool.

For more information, please refer to "*How Do I Remove The Shield Deluxe Completely?*" (p. 140).

If this information was not helpful, you can contact us for support as described in section "*Support*" (p. 137).

29. Removing Malware from Your System

Malware can affect your system in many different ways and SHIELD DELUXE 2013 approach depends on the type of malware attack. Because viruses change their behavior frequently, it is difficult to establish a pattern for their behavior and their actions.

There are situations when SHIELD DELUXE 2013 cannot automatically remove the malware infection from your system. In such cases, your intervention is required.

If you cannot find your problem here, or if the presented solutions do not solve it, you can contact the PCSecurityShield technical support representatives as presented in chapter "*Support*" (p. 137).

29.1. What to Do When SHIELD DELUXE 2013 Finds Viruses on Your Computer?

You may find out there is a virus on your computer in one of these ways:

- You scanned your computer and SHIELD DELUXE 2013 found infected items on it.
- A virus alert informs you that SHIELD DELUXE 2013 blocked one or multiple viruses on your computer.

In such situations, update SHIELD DELUXE 2013 to make sure you have the latest malware signatures and run a Deep System Scan to analyze the system.

As soon as the deep scan is over, select the desired action for the infected items (Disinfect, Delete, Move to quarantine).

If the selected action could not be taken and the scan log reveals an infection which could not be deleted, you have to remove the file(s) manually:

The first method can be used in Normal mode:

1. Turn off SHIELD DELUXE 2013 real-time antivirus protection. To find out how to do this, please refer to "*How Do I Enable / Disable the Real Time Protection?*" (p. 141).
2. Display hidden objects in Windows. To find out how to do this, please refer to "*How Do I Display Hidden Objects in Windows?*" (p. 142).
3. Browse to the location of the infected file (check the scan log) and delete it.

4. Turn on SHIELD DELUXE 2013 real-time antivirus protection.

In case the first method failed to remove the infection, follow these steps:

1. Reboot your system and enter in Safe Mode. To find out how to do this, please refer to "*How Do I Restart in Safe Mode?*" (p. 139).
2. Display hidden objects in Windows.
3. Browse to the location of the infected file (check the scan log) and delete it.
4. Reboot your system and enter in normal mode.

If this information was not helpful, you can contact us for support as described in section "*Support*" (p. 137).

29.2. How Do I Clean a Virus in an Archive?

An archive is a file or a collection of files compressed under a special format to reduce the space on disk necessary for storing the files.

Some of these formats are open formats, thus providing SHIELD DELUXE 2013 the option to scan inside them and then take appropriate actions to remove them.

Other archive formats are partially or fully closed, and SHIELD DELUXE 2013 can only detect the presence of viruses inside them, but is not able to take any other actions.

If SHIELD DELUXE 2013 notifies you that a virus has been detected inside an archive and no action is available, it means that removing the virus is not possible due to restrictions on the archive's permission settings.

Here is how you can clean a virus stored in an archive:

1. Identify the archive that includes the virus by performing a Deep System Scan of the system.
2. Turn off SHIELD DELUXE 2013 real-time antivirus protection.
3. Go to the location of the archive and decompress it using an archiving application, like WinZip.
4. Identify the infected file and delete it.
5. Delete the original archive in order to make sure the infection is totally removed.
6. Recompress the files in a new archive using an archiving application, like WinZip.

7. Turn on SHIELD DELUXE 2013 real-time antivirus protection and run a Deep system scan in order to make sure there is no other infection on the system.

> *Note*
> It's important to note that a virus stored in an archive is not an immediate threat to your system, since the virus has to be decompressed and executed in order to infect your system.

If this information was not helpful, you can contact us for support as described in section "*Support*" (p. 137).

29.3. How Do I Clean a Virus in an E-Mail Archive?

SHIELD DELUXE 2013 can also identify viruses in e-mail databases and e-mail archives stored on disk.

Sometimes it is necessary to identify the infected message using the information provided in the scan report, and delete it manually.

Here is how you can clean a virus stored in an e-mail archive:

1. Scan the e-mail database with SHIELD DELUXE 2013.
2. Turn off SHIELD DELUXE 2013 real-time antivirus protection.
3. Open the scan report and use the identification information (Subject, From, To) of the infected messages to locate them in the e-mail client.
4. Delete the infected messages. Most e-mail clients also move the deleted message to a recovery folder, from which it can be recovered. You should make sure the message is deleted also from this recovery folder.
5. Compact the folder storing the infected message.
   - In Outlook Express: On the File menu, click Folder, then Compact All Folders.
   - In Microsoft Outlook: On the File menu, click Data File Management. Select the personal folders (.pst) files you intend to compact, and click Settings. Click Compact.
6. Turn on SHIELD DELUXE 2013 real-time antivirus protection.

If this information was not helpful, you can contact us for support as described in section "*Support*" (p. 137).

29.4. What to Do When SHIELD DELUXE 2013 Detected a Clean File as Infected?

There are cases when SHIELD DELUXE 2013 mistakenly flags a legitimate file as being a threat (a false positive). To correct this error, add the file to SHIELD DELUXE 2013 Exclusions area:

1. Turn off SHIELD DELUXE 2013 real-time antivirus protection. To find out how to do this, please refer to "*How Do I Enable / Disable the Real Time Protection?*" (p. 141).
2. Display hidden objects in Windows. To find out how to do this, please refer to "*How Do I Display Hidden Objects in Windows?*" (p. 142).
3. Restore the file from the Quarantine area.
4. Insert the file in the Exclusions area.
5. Turn on SHIELD DELUXE 2013 real-time antivirus protection.

If this information was not helpful, you can contact us for support as described in section "*Support*" (p. 137).

29.5. How to Clean the Infected Files from System Volume Information

The System Volume Information folder is a zone on your hard drive created by the Operating System and used by Windows for storing critical information related to the system configuration.

SHIELD DELUXE 2013 engines can detect any infected files stored by the System Volume Information, but being a protected area it may not be able to remove them.

The infected files detected in the System Restore folders will appear in the scan log as follows:

```
?:\System Volume Information\_restore{B36120B2-BA0A-4E5D-…
```

To completely and immediately remove the infected file or files in the data store, disable and re-enable the System Restore feature.

When System Restore is turned off, all the restore points are removed.

When System Restore is turned on again, new restore points are created as the schedule and events require.

In order to disable the System Restore follow these steps:

- **For Windows XP:**
  1. Follow this path: **Start** → **All Programs** → **Accessories** → **System Tool** → **System Restore**
  2. Click **System Restore Settings** located on the left hand side of the window.
  3. Select the **Turn off System Restore** check box on all drives, and click **Apply**.
  4. When you are warned that all existing Restore Points will be deleted, click **Yes** to continue.
  5. To turn on the System Restore, clear the **Turn off System Restore** check box on all drives, and click **Apply**.
- **For Windows Vista:**
  1. Follow this path: **Start** → **Control Panel** → **System and Maintenance** → **System**
  2. In the left pane, click **System Protection**.

     If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
  3. To turn off the System Restore clear the check boxes corresponding to each drive and click **Ok**.
  4. To turn on the System Restore select the check boxes corresponding to each drive and click **Ok**.
- **For Windows 7:**
  1. Click **Start**, right-click **Computer** and click **Properties**.
  2. Click **System protection** link in the left pane.
  3. In the **System protection** options, select each drive letter and click **Configure**.
  4. Select **Turn off system protection** and click **Apply**.
  5. Click **Delete**, click **Continue** when prompted and then click **Ok**.

If this information was not helpful, you can contact us for support as described in section "*Support*" (p. 137).

29.6. What Are the Password-Protected Files in the Scan Log?

This is only a notification which indicates that SHIELD DELUXE 2013 has detected these files are either protected with a password or by some form of encryption.

Most commonly, the password-protected items are:

- Files that belong to another security solution.
- Files that belong to the operating system.

In order to actually scan the contents, these files would need to either be extracted or otherwise decrypted.

Should those contents be extracted, SHIELD DELUXE 2013's real-time scanner would automatically scan them to keep your computer protected. If you want to scan those files with SHIELD DELUXE 2013, you have to contact the product manufacturer in order to provide you with more details on those files.

Our recommendation to you is to ignore those files because they are not a threat for your system.

29.7. What Are the Skipped Items in the Scan Log?

All files that appear as Skipped in the scan report are clean.

For increased performance, SHIELD DELUXE 2013 does not scan files that have not changed since the last scan.

29.8. What Are the Over-Compressed Files in the Scan Log?

The over-compressed items are elements which could not be extracted by the scanning engine or elements for which the decryption time would have taken too long making the system unstable.

Overcompressed means that SHIELD DELUXE 2013 skipped scanning within that archive because unpacking it proved to take up too many system resources. The content will be scanned on real time access if needed.

29.9. Why Did SHIELD DELUXE 2013 Automatically Delete an Infected File?

If an infected file is detected, SHIELD DELUXE 2013 will automatically attempt to disinfect it. If disinfection fails, the file is moved to quarantine in order to contain the infection.

For particular types of malware, disinfection is not possible because the detected file is entirely malicious. In such cases, the infected file is deleted from the disk.

This is usually the case with installation files that are downloaded from untrustworthy websites. If you find yourself in such a situation, download the installation file from the manufacturer's website or other trusted website.

30. Support

If you need help or additional information on SHIELD DELUXE 2013, use the contact information provided below.

PCSecurityShield
601 N Congress Avenue
Suite 303
Delray Beach, FL 33445
Phone: 561-243-3247
Fax: 561-243-3249
Buy: http://renew.pcsecurityshield.com/bsd10/activate.aspx
Renew: http://renew.pcsecurityshield.com/bsd10/renew.aspx
FAQ Web Page: http://support.pcsecurityshield.com/faq/FAQs.asp
Technical Support: http://support.pcsecurityshield.com/
Product Website: http://www.PCSecurityShield.com

31. Useful Information

This chapter presents some important procedures that you must be aware before starting to troubleshoot a technical issue.

Troubleshooting a technical situation in SHIELD DELUXE 2013 requires a few Windows insights, therefore the next steps are mostly related to the Windows operating system.

31.1. How Do I Remove Other Security Solutions?

The main reason for using a security solution is to provide protection and safety for your data. But what happens when you have more than one security product on the same system?

When you use more than one security solution on the same computer, the system becomes unstable. SHIELD DELUXE 2013 2013 installer automatically detects other security programs and offers you the option to uninstall them.

If you did not remove the other security solutions during the initial installation, follow these steps:

- For **Windows XP**:
  1. Click **Start**, go to **Control Panel** and double-click **Add / Remove programs**.
  2. Wait a few moments until the list of installed software is displayed.
  3. Find the name of the program you want to remove and select **Remove**.
  4. Wait for the uninstall process to complete, then reboot your system.
- For **Windows Vista** and **Windows 7**:
  1. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.
  2. Wait a few moments until the installed software list is displayed.
  3. Find the name of the program you want to remove and select **Uninstall**.
  4. Wait for the uninstall process to complete, then reboot your system.

If you fail to remove the other security solution from your system, get the uninstall tool from the vendor website or contact them directly in order to provide you with the uninstall guidelines.

31.2. How Do I Restart in Safe Mode?

Safe mode is a diagnostic operating mode, used mainly to troubleshoot problems affecting normal operation of Windows. Such problems range from conflicting drivers to viruses preventing Windows from starting normally. In Safe Mode only a few applications work and Windows loads just the basic drivers and a minimum of operating system components. This is why most viruses are inactive when using Windows in Safe Mode and they can be easily removed.

To start Windows in Safe Mode:

1. Restart the computer.
2. Press the **F8** key several times before Windows starts in order to access the boot menu.
3. Select **Safe Mode** in the boot menu and press **Enter**.
4. Wait while Windows loads in Safe Mode.
5. This process ends with a confirmation message. Click **Ok** to acknowledge.
6. To start Windows normally, simply reboot the system.

31.3. Am I Using a 32 bit or a 64 bit Version of Windows?

To find out if you have a 32 bit or a 64 bit operating system, follow these steps:

- For **Windows XP**:
  1. Click **Start**.
  2. Locate **My Computer** on the **Start** menu.
  3. Right-click **My Computer** and select **Properties**.
  4. If you see **x64 Edition** listed under **System**, you are running the 64 bit version of Windows XP.

     If you don't see **x64 Edition** listed, you are running a 32 bit version of Windows XP.
- For **Windows Vista** and **Windows 7**:
  1. Click **Start**.

2. Locate **Computer** on the **Start** menu.
3. Right-click **Computer** and select **Properties**.
4. Look under **System** in order to check the information about your system.

31.4. How Do I Find Out My Proxy Settings?

In order to find these settings, follow these steps :

- For Internet Explorer 8:
  1. Open Internet Explorer.
  2. Select **Tools** > **Internet Options**.
  3. In the **Connections** tab click **LAN settings**.
  4. Look under **Use a proxy server for your LAN** and you should see the **Address** and **Port** of the proxy.
- For Mozilla Firefox 3.6:
  1. Open Firefox.
  2. Select **Tools** > **Options**.
  3. In the **Advanced** tab go to **Network** tab.
  4. Click **Settings**.
- For Opera 10.51:
  1. Open Opera.
  2. Select **Tools** > **Preferences**.
  3. In the **Advanced** tab go to **Network** tab.
  4. Click **Proxy servers** button to open the proxy settings dialog.

31.5. How Do I Remove SHIELD DELUXE 2013 Completely?

Follow these steps in order to remove SHIELD DELUXE 2013 correctly:

1. Contact the PCSecurityShield technical support as described in "*Support*" (p. 137) and ask for the uninstall tool.

2. Run the uninstall tool using administrator privileges.
3. Restart your computer.

31.6. How Do I Enable / Disable the Real Time Protection?

SHIELD DELUXE 2013 provides continuous, real-time protection against a wide range of malware threats by scanning all accessed files, e-mail messages and the communications through Instant Messaging Software applications (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

Normally the real-time protection in SHIELD DELUXE 2013 is enabled and you should not turn it off.

When you are trying to troubleshoot a problem or to remove a virus, you may need to disable the real-time protection. They address one of these situations:

- A slowdown issue with the system after installing SHIELD DELUXE 2013
- An issue with one of the programs or applications after installing SHIELD DELUXE 2013
- Error messages which could appear shortly after installing SHIELD DELUXE 2013

Follow these steps so that you may enable/ disable real-time protection temporarily:

1. Open SHIELD DELUXE 2013, click **Options** in the upper-right corner of the window and choose **Expert View**.
2. Go to **Antivirus** > **Shield**.
3. Clear the **Real-time protection is enabled** check box to temporarily disable antivirus protection (or select it if you want to enable the protection).
4. You must confirm your choice by selecting from the menu how long you want the real-time protection to be disabled.

Note

The steps for disabling the real-time protection in SHIELD DELUXE 2013 should be used as a temporary solution and only for a short period of time.

31.7. How Do I Display Hidden Objects in Windows?

These steps are useful in those cases where you are dealing with a malware situation and you need to find and remove the infected files, which could be hidden.

Follow these steps to display hidden objects in Windows:

1. Click **Start**, go to **Control Panel** and select **Folder Options**.
2. Go to **View** tab.
3. Select **Display contents of system folders** (for Windows XP only).
4. Select **Show hidden files and folders**.
5. Clear **Hide file extensions for known file types**.
6. Clear **Hide protected operating system files**.
7. Click **Apply** and then **Ok**.

Glossary

ActiveX

ActiveX is a model for writing programs so that other programs and the operating system can call them. ActiveX technology is used with Microsoft Internet Explorer to make interactive Web pages that look and behave like computer programs, rather than static pages. With ActiveX, users can ask or answer questions, use push buttons, and interact in other ways with the Web page. ActiveX controls are often written using Visual Basic.

Active X is notable for a complete lack of security controls; computer security experts discourage its use over the Internet.

Adware

Adware is often combined with a host application that is provided at no charge as long as the user agrees to accept the adware. Because adware applications are usually installed after the user has agreed to a licensing agreement that states the purpose of the application, no offense is committed.

However, pop-up advertisements can become an annoyance, and in some cases degrade system performance. Also, the information that some of these applications collect may cause privacy concerns for users who were not fully aware of the terms in the license agreement.

Archive

A disk, tape, or directory that contains files that have been backed up.

A file that contains one or more files in a compressed format.

Backdoor

A hole in the security of a system deliberately left in place by designers or maintainers. The motivation for such holes is not always sinister; some operating systems, for example, come out of the box with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers.

Boot sector

A sector at the beginning of each disk that identifies the disk's architecture (sector size, cluster size, and so on). For startup disks, the boot sector also contains a program that loads the operating system.

Boot virus

A virus that infects the boot sector of a fixed or floppy disk. An attempt to boot from a diskette infected with a boot sector virus will cause the virus to become active in memory. Every time you boot your system from that point on, you will have the virus active in memory.

Browser

Short for Web browser, a software application used to locate and display Web pages. The two most popular browsers are Netscape Navigator and Microsoft Internet Explorer. Both of these are graphical browsers, which means that they can display graphics as well as text. In addition, most modern browsers can present multimedia information, including sound and video, though they require plug-ins for some formats.

Command line

In a command line interface, the user types commands in the space provided directly on the screen using command language.

Cookie

Within the Internet industry, cookies are described as small files containing information about individual computers that can be analyzed and used by advertisers to track your online interests and tastes. In this realm, cookie technology is still being developed and the intention is to target ads directly to what you've said your interests are. It's a double-edge sword for many people because on one hand, it's efficient and pertinent as you only see ads about what you're interested in. On the other hand, it involves actually "tracking" and "following" where you go and what you click. Understandably so, there is a debate over privacy and many people feel offended by the notion that they are viewed as a "SKU number" (you know, the bar code on the back of packages that gets scanned at the grocery check-out line). While this viewpoint may be extreme, in some cases it is accurate.

Disk drive

It's a machine that reads data from and writes data onto a disk.

A hard disk drive reads and writes hard disks.

A floppy drive accesses floppy disks.

Disk drives can be either internal (housed within a computer) or external (housed in a separate box that connects to the computer).

Download

To copy data (usually an entire file) from a main source to a peripheral device. The term is often used to describe the process of copying a file from an online service to one's own computer. Downloading can also refer to copying a file from a network file server to a computer on the network.

E-mail

Electronic mail. A service that sends messages on computers via local or global networks.

Events

An action or occurrence detected by a program. Events can be user actions, such as clicking a mouse button or pressing a key, or system occurrences, such as running out of memory.

False positive

Occurs when a scanner identifies a file as infected when in fact it is not.

Filename extension

The portion of a filename, following the final point, which indicates the kind of data stored in the file.

Many operating systems use filename extensions, e.g. Unix, VMS, and MS-DOS. They are usually from one to three letters (some sad old OSes support no more than three). Examples include "c" for C source code, "ps" for PostScript, "txt" for arbitrary text.

Heuristic

A rule-based method of identifying new viruses. This method of scanning does not rely on specific virus signatures. The advantage of the heuristic scan is that it is not fooled by a new variant of an existing virus. However, it might occasionally report suspicious code in normal programs, generating the so-called "false positive".

IP

Internet Protocol - A routable protocol in the TCP/IP protocol suite that is responsible for IP addressing, routing, and the fragmentation and reassembly of IP packets.

Java applet

A Java program which is designed to run only on a web page. To use an applet on a web page, you would specify the name of the applet and the size (length and width, in pixels) that the applet can utilize. When the web page is accessed, the browser downloads the applet from a server and runs it on the user's machine (the client). Applets differ from applications in that they are governed by a strict security protocol.

For example, even though applets run on the client, they cannot read or write data onto the client's machine. Additionally, applets are further restricted so that they can only read and write data from the same domain that they are served from.

Macro virus

A type of computer virus that is encoded as a macro embedded in a document. Many applications, such as Microsoft Word and Excel, support powerful macro languages.

These applications allow you to embed a macro in a document, and have the macro execute each time the document is opened.

Mail client

An e-mail client is an application that enables you to send and receive e-mail.

Memory

Internal storage areas in the computer. The term memory identifies data storage that comes in the form of chips, and the word storage is used for memory that exists on tapes or disks. Every computer comes with a certain amount of physical memory, usually referred to as main memory or RAM.

Non-heuristic

This method of scanning relies on specific virus signatures. The advantage of the non-heuristic scan is that it is not fooled by what might seem to be a virus, and does not generate false alarms.

Packed programs

A file in a compression format. Many operating systems and applications contain commands that enable you to pack a file so that it takes up less memory. For example, suppose you have a text file containing ten consecutive space characters. Normally, this would require ten bytes of storage.

However, a program that packs files would replace the space characters by a special space-series character followed by the number of spaces being replaced. In this case, the ten spaces would require only two bytes. This is just one packing technique - there are many more.

Path

The exact directions to a file on a computer. These directions are usually described by means of the hierarchical filing system from the top down.

The route between any two points, such as the communications channel between two computers.

Phishing

The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

Polymorphic virus

A virus that changes its form with each file it infects. Since they have no consistent binary pattern, such viruses are hard to identify.

Port

An interface on a computer to which you can connect a device. Personal computers have various types of ports. Internally, there are several ports for connecting disk drives, display screens, and keyboards. Externally, personal computers have ports for connecting modems, printers, mice, and other peripheral devices.

In TCP/IP and UDP networks, an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

Report file

A file that lists actions that have occurred. SHIELD DELUXE 2013 maintains a report file listing the path scanned, the folders, the number of archives and files scanned, how many infected and suspicious files were found.

Rootkit

A rootkit is a set of software tools which offer administrator-level access to a system. The term was first used for the UNIX operating systems and it referred to recompiled tools which provided intruders administrative rights, allowing them to conceal their presence so as not to be seen by the system administrators.

The main role of rootkits is to hide processes, files, logins and logs. They may also intercept data from terminals, network connections or peripherals, if they incorporate the appropriate software.

Rootkits are not malicious in nature. For example, systems and even some applications hide critical files using rootkits. However, they are mostly used to hide malware or to conceal the presence of an intruder into the system. When combined with malware, rootkits pose a great threat to the integrity and the security of a system. They can monitor traffic, create backdoors into the system, alter files and logs and avoid detection.

Script

Another term for macro or batch file, a script is a list of commands that can be executed without user interaction.

Spam

Electronic junk mail or junk newsgroup postings. Generally known as any unsolicited e-mail.

Spyware

Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.

Spyware's similarity to a Trojan horse is the fact that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today.

Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's Internet connection. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability.

Startup items

Any files placed in this folder will open when the computer starts. For example, a startup screen, a sound file to be played when the computer first starts, a reminder calendar, or application programs can be startup items. Normally, an alias of a file is placed in this folder rather than the file itself.

System tray

Introduced with Windows 95, the system tray is located in the Windows taskbar (usually at the bottom next to the clock) and contains miniature icons for easy access to system functions such as fax, printer, modem, volume, and more. Double click or right-click an icon to view and access the details and controls.

TCP/IP

Transmission Control Protocol/Internet Protocol - A set of networking protocols widely used on the Internet that provides communications across interconnected networks of computers with diverse hardware architectures and various operating systems. TCP/IP includes standards for how computers communicate and conventions for connecting networks and routing traffic.

Trojan

A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

The term comes from a story in Homer's Iliad, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

Update

A new version of a software or hardware product designed to replace an older version of the same product. In addition, the installation routines for updates often check to make sure that an older version is already installed on your computer; if not, you cannot install the update.

SHIELD DELUXE 2013 has it's own update module that allows you to manually check for updates, or let it automatically update the product.

Virus

A program or piece of code that is loaded onto your computer without your knowledge and runs against your will. Most viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can copy itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

Virus definition

The binary pattern of a virus, used by the antivirus program to detect and eliminate the virus.

Worm

A program that propagates itself over a network, reproducing itself as it goes. It cannot attach itself to other programs.